日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年　６月１５日

出願番号
Application Number: 平成１１年特許願第１６７８９８号

出願人
Applicant (s): 松下電器産業株式会社

２０００年　６月　２日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号　出証特２０００－３０４１２２３

【書類名】　特許願

【整理番号】　2022510286

【提出日】　平成11年 6月15日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 9/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　茨木　晋

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　勝田　昇

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　館林　誠

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　井上　信治

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【プルーフの要否】　不要

【書類名】　明細書

【発明の名称】　暗号処理装置、暗号処理方法および記録媒体

【特許請求の範囲】

【請求項１】暗号処理を行う領域を記述する動作記述情報で特定された領域に暗号化あるいは復号化の暗号処理を行うことを特徴とする暗号処理装置であって、

前記動作記述情報は、コンテンツ中の同期情報の長さを示す情報と同期情報のパターンを示す情報を少なくとも持つ同期記述情報を有し、

前記同期記述情報により記述される同期情報をコンテンツから探索することを特徴とする同期検出装置を有することを特徴とする暗号処理装置。

【請求項２】前記動作記述情報は同期記述情報と共に使用される同期検出命令および同期検証命令を含み、

前記同期検出装置が、前記同期検出命令によって同期情報を探索し、前記同期検証命令によって終了位置後の同期情報が正しいかどうかを検証することを特徴とする請求項２記載の暗号処理装置。

【請求項３】暗号処理を行う領域を記述する動作記述情報で特定された領域に暗号化あるいは復号化の暗号処理を行うことを特徴とする暗号処理装置であって、

前記動作記述情報は、コンテンツ中の長さを示すコード位置を特定する情報と前記コードのビット長を特定する領域記述情報を含み、

前記領域記述情報により記述されるコードをコンテンツ中から抜き出し、前記コードから位置を示す情報を算出する領域検出装置を有することを特徴とする暗号処理装置。

【請求項４】前記領域記述情報が２のべき乗で表現される単位長情報を含み、

前記領域検出装置が前記長さを示すコードに対して単位長情報のビットシフトを行うことを特徴とする請求項３記載の暗号処理装置。

【請求項５】前記領域検出装置が、暗号処理を開始する位置あるいは暗号処理を終了する位置を特定することを特徴とする請求項４記載の暗号処理装置。

【請求項６】暗号処理を行う領域を記述する動作記述情報で特定された領域に

暗号化あるいは復号化の暗号処理を行うことを特徴とする暗号処理装置であって、

前記動作記述情報は、暗号化処理の方法を特定する情報を含む暗号記述情報を含み、

暗号処理を行う領域を特定する情報を入力とし、前記暗号処理を行う領域に前記暗号記述情報で特定される暗号処理を施す暗号処理部を具備することを特徴とする暗号処理装置。

【請求項７】前記暗号記述情報が、基本暗号情報と一つ以上のオプション暗号情報から構成され、前記それぞれのオプション暗号情報は、オプションの暗号処理の方法を特定する情報と、前記オプションの適用される範囲を示す情報を含み、

前記暗号処理部は、前記暗号処理を行う領域を基本暗号あるいはオプション暗号によって暗号処理することを特徴とする請求項６記載の暗号処理装置。

【請求項８】暗号処理を行う領域を記述する動作記述情報を入力とし、

前記動作記述情報で記述された領域に暗号化あるいは復号化の暗号処理を行うことを特徴とする暗号処理装置において、

前記動作記述情報は、コンテンツ中の同期情報の長さを示す情報と同期情報のパターンを示す情報を少なくとも持つ同期記述情報と、コンテンツ中の長さを示すコード位置を特定する情報と前記コードのビット長を特定する領域記述情報と、暗号化処理の方法を特定する情報を含む暗号記述情報を含み、

前記同期記述情報により記述される同期情報をコンテンツから探索することを特徴とする同期検出装置と、

前記領域記述情報により記述されるコードをコンテンツ中から抜き出し、前記コードから位置を示す情報を算出することを特徴とする領域検出部と、

暗号処理を行う領域を特定する情報を入力とし、前記暗号処理を行う領域に前記暗号記述情報で特定される暗号処理を施す暗号処理部を具備することを特徴とする暗号処理装置。

【請求項９】前記領域検出部が、暗号処理を行う領域を検出することを特徴とする請求項８記載の暗号処理装置。

【請求項１０】前記動作記述情報が命令の組み合わせであり、

前記動作記述情報により記述される順番で、前記同期検出部、前記領域検出部、および前記暗号処理部の処理を制御するプロセッサを有する請求項８記載の暗号処理装置。

【請求項１１】前記動作記述情報が、前記同期記述情報、前記領域記述情報、前記暗号記述情報の組み合わせで構成されており、

前記同期検出部、前記領域検出部、および前記暗号処理部が規定の順番で処理を行うことを特徴とする請求項１０記載の暗号処理装置。

【請求項１２】暗号処理を行う領域を記述する動作記述情報で特定された領域に暗号化あるいは復号化の暗号処理を行うことを特徴とする暗号処理方法であって、

前記動作記述情報は、コンテンツ中の同期情報の長さを示す情報と同期情報のパターンを示す情報を少なくとも持つ同期記述情報を有し、

前記同期記述情報により記述される同期情報をコンテンツから探索する手順を有することを特徴とする暗号処理方法。

【請求項１３】前記動作記述情報は同期記述情報と共に使用される同期検出命令および同期検証命令を含み、

前記同期検出命令によって同期情報を探索する手順と、前記同期検証命令によって終了位置後の同期情報が正しいかどうかを検証する手順を有することを特徴とする請求項１２記載の暗号処理方法。

【請求項１４】暗号処理を行う領域を記述する動作記述情報で特定された領域に暗号化あるいは復号化の暗号処理を行うことを特徴とする暗号処理方法であって、

前記動作記述情報は、コンテンツ中の長さを示すコード位置を特定する情報と前記コードのビット長を特定する領域記述情報を含み、

前記領域記述情報により記述されるコードをコンテンツ中から抜き出し、前記コードから位置を示す情報を算出する手順を有することを特徴とする暗号処理方法。

【請求項１５】前記領域記述情報が２のべき乗で表現される単位長情報を含み

前記長さを示すコードに対して単位長情報のビットシフトを行う手順を有することを特徴とする請求項１４記載の暗号処理方法。

【請求項１６】暗号処理を開始する位置あるいは暗号処理を終了する位置を特定する手順を有することを特徴とする請求項１５記載の暗号処理方法。

【請求項１７】暗号処理を行う領域を記述する動作記述情報で特定された領域に暗号化あるいは復号化の暗号処理を行うことを特徴とする暗号処理方法であって、

前記動作記述情報は、暗号化処理の方法を特定する情報を含む暗号記述情報を含み、

暗号処理を行う領域を特定する情報を入力とし、前記暗号処理を行う領域に前記暗号記述情報で特定される暗号処理を施す手順を有することを特徴とする暗号処理方法。

【請求項１８】前記暗号記述情報が、基本暗号情報と一つ以上のオプション暗号情報から構成され、前記それぞれのオプション暗号情報は、オプションの暗号処理の方法を特定する情報と、前記オプションの適用される範囲を示す情報を含み、

前記暗号処理を行う領域を基本暗号あるいはオプション暗号によって処理するかを前記範囲を示す情報から判定する手順を有することを特徴とする請求項１７記載の暗号処理方法。

【請求項１９】暗号処理を行う領域を記述する動作記述情報で特定された領域に暗号化あるいは復号化の暗号処理を行うことを特徴とする暗号処理方法において、

前記動作記述情報は、コンテンツ中の同期情報の長さを示す情報と同期情報のパターンを示す情報を少なくとも持つ同期記述情報と、コンテンツ中の長さを示すコード位置を特定する情報と前記コードのビット長を特定する領域記述情報と、暗号化処理の方法を特定する情報を含む暗号記述情報を含み、

前記同期記述情報により記述される同期情報をコンテンツから探索する手順と、

前記領域記述情報により記述されるコードをコンテンツ中から抜き出し、前記コードから位置を示す情報を算出する手順と、

暗号処理を行う領域を特定する情報を入力とし、前記暗号処理を行う領域に前記暗号記述情報で特定される暗号処理を施す手順と、を有することを特徴とする暗号処理方法。

【請求項２０】前記位置を算出する手順を用いて、暗号処理を行う領域を検出することを特徴とする請求項１９記載の暗号処理方法。

【請求項２１】前記動作記述情報が命令の組み合わせであり、

前記動作記述情報により記述される順番で、各手順の処理を行うことを特徴とする請求項１９記載の暗号処理装置。

【請求項２２】前記動作記述情報が、前記同期記述情報、前記領域記述情報、前記暗号記述情報の組み合わせで構成されており、

規定の順番で前記各手順を行うことを特徴とする請求項１９記載の暗号処理装置。

【請求項２３】コンテンツ中の同期情報の長さを示す情報と同期情報のパターンを示す情報を少なくとも持つ同期記述情報と、コンテンツ中の長さを示すコード位置を特定する情報と前記コードのビット長を特定する領域記述情報と、暗号化処理の方法を特定する情報を含む暗号記述情報のうち少なくとも一つからなる動作記述情報を記録する記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、任意のフォーマットのコンテンツに、暗号化やその復号化などの暗号処理を行う、暗号処理装置および暗号処理方法と、任意のフォーマットのコンテンツの暗号処理の方法を記述した動作記述情報を記録する記録媒体に関する。

【０００２】

【従来の技術】

従来の暗号処理装置の動作を図１６を用いて説明する。

【０００３】

従来の暗号処理装置においては、図１６（ａ）に示すように、固定長パケットから構成されるコンテンツを処理していた。この従来の暗号処理装置は、図に示すようにコンテンツ中から既定の同期パターンを検出し、同期パターンを除く既定の部分に暗号処理を施していた。

【０００４】

また、別の従来の暗号処理装置においては、図１６（ｂ）に示すように、可変長パケットから構成されるコンテンツを処理していた。この従来の暗号処理装置は、図に示すように、コンテンツ中から既定の同期パターンを検出し、その後コンテンツ中の既定の位置からパケット長を示すレングスを抜き出し、パケットの長さを検出していた。その後、同期パターンおよびレングスを除く既定の部分に暗号処理を施していた。

【０００５】

また、別の従来の暗号処理装置においては、図１６（ｃ）に示すように、コンテンツのフォーマットに関係なく、一定の周期で暗号処理を施していた。

【０００６】

【発明が解決しようとする課題】

しかるに、従来の暗号処理装置においては、コンテンツのフォーマットや暗号処理の方法によって、個別に処理の方法を決定し、個別の装置を構成しなければならないという課題があった。

【０００７】

本発明の目的は、従来の暗号処理装置の課題を解決し、一つの暗号処理装置によって複数の任意のフォーマットのコンテンツを処理可能な暗号処理装置を構成することである。

【０００８】

【課題を解決するための手段】

以上の課題を解決するために、本発明（請求項１）の暗号処理装置は、動作記述情報で特定された領域に暗号化あるいは復号化の暗号処理を行う暗号処理装置であって、コンテンツ中の同期情報の長さを示す情報と同期情報のパターンを示す情報を少なくとも持つ同期記述情報により記述される同期情報をコンテンツか

ら探索する同期検出装置を有するものである。

【０００９】

また、本発明（請求項２）の暗号処理装置は、請求項１記載の暗号処理装置において、前記動作記述情報が同期検出命令および同期検証命令を含み、前記同期検出部が、前記同期検出命令によって同期情報を探索し、前記同期検証命令によって終了位置後の同期情報が正しいかどうかを検証するものである。

【００１０】

また、本発明（請求項３）の暗号処理装置は、動作記述情報で特定された領域に暗号化あるいは復号化の暗号処理を行う暗号処理装置であって、コンテンツ中の長さを示すコードの位置を特定する情報と前記コードのビット長を特定する領域記述情報を含み、前記領域記述情報により記述されるコードをコンテンツ中から抜き出し、前記コードから位置を示す情報を算出する領域検出装置を有するものである。

【００１１】

また、本発明（請求項４）の暗号処理装置は、請求項３記載の暗号処理装置であって、前記領域記述情報が２のべき乗で表現される単位長情報を含み、前記領域検出装置が前記長さを示すコードに対して単位長情報のビットシフトを行うものである。

【００１２】

また、本発明（請求項５）の暗号処理装置は、請求項３記載の暗号処理装置であって、前記領域検出装置が、暗号処理を開始する位置あるいは暗号処理を終了する位置を特定するものである。

【００１３】

また、本発明（請求項６）の暗号処理装置は、動作記述情報で特定された領域に暗号化あるいは復号化の暗号処理を行うことを特徴とする暗号処理装置であって、前記動作記述情報は、暗号化処理の方法を特定する情報を含む暗号記述情報を含み、暗号処理を行う領域を特定する情報を入力とし、前記暗号処理を行う領域に前記暗号記述情報で特定される暗号処理を施す暗号処理部を具備するものである。

【００１４】

また、本発明（請求項７）の暗号処理装置は、請求項６記載の暗号処理装置であって、前記暗号記述情報が、基本暗号情報と一つ以上のオプション暗号情報から構成され、前記それぞれのオプション暗号情報は、オプションの暗号処理の方法を特定する情報と、前記オプションの適用される範囲を示す情報を含み、前記暗号処理部は、前記暗号処理を行う領域を基本暗号あるいはオプション暗号によって暗号処理するものである。

【００１５】

また、本発明（請求項８）の暗号処理装置は、動作記述情報で記述された領域に暗号化あるいは復号化の暗号処理を行うことを特徴とする暗号処理装置において、前記動作記述情報は、コンテンツ中の同期情報の長さを示す情報と同期情報のパターンを示す情報を少なくとも持つ同期記述情報と、コンテンツ中の長さを示すコード位置を特定する情報と前記コードのビット長を特定する領域記述情報と、暗号化処理の方法を特定する情報を含む暗号記述情報を含み、前記同期記述情報により記述される同期情報をコンテンツから探索することを特徴とする同期検出装置と、前記領域記述情報により記述されるコードをコンテンツ中から抜き出し、前記コードから位置を示す情報を算出することを特徴とする領域検出部と、暗号処理を行う領域を特定する情報を入力とし、前記暗号処理を行う領域に前記暗号記述情報で特定される暗号処理を施す暗号処理部を具備するものである。

【００１６】

また、本発明（請求項９）の暗号処理装置は、請求項８記載の暗号処理装置であって、前記領域検出部が、暗号処理を行う領域を検出するものである。

【００１７】

また、本発明（請求項１０）の暗号処理装置は、請求項８記載の暗号処理装置であって、前記動作記述情報が命令の組み合わせであり、前記動作記述情報により記述される順番で、前記同期検出部、前記領域検出部、および前記暗号処理部の処理を制御するプロセッサを有するものである。

【００１８】

また、本発明（請求項１１）の暗号処理装置は、請求項８記載の暗号処理装置

であって、前記動作記述情報が、前記同期記述情報、前記領域記述情報、前記暗号記述情報の組み合わせで構成されており、前記同期検出部、前記領域検出部、および前記暗号処理部が規定の順番で処理を行うものである。

【００１９】

また、本発明（請求項１２）の暗号処理方法は、動作記述情報で特定された領域に暗号化あるいは復号化の暗号処理を行うことを特徴とする暗号処理方法であって、前記動作記述情報は、コンテンツ中の同期情報の長さを示す情報と同期情報のパターンを示す情報を少なくとも持つ同期記述情報を有し、前記同期記述情報により記述される同期情報をコンテンツから探索する手順を有するものである。

【００２０】

また、本発明（請求項１３）の暗号処理方法は、請求項１２記載の暗号処理方法であって、前記動作記述情報は同期記述情報と共に使用される同期検出命令および同期検証命令を含み、前記同期検出命令によって同期情報を探索する手順と、前記同期検証命令によって終了位置後の同期情報が正しいかどうかを検証する手順を有することを特徴とするものである。

【００２１】

また、本発明（請求項１４）の暗号処理方法は、動作記述情報で特定された領域に暗号化あるいは復号化の暗号処理を行うことを特徴とする暗号処理方法であって、前記動作記述情報は、コンテンツ中の長さを示すコード位置を特定する情報と前記コードのビット長を特定する領域記述情報を含み、前記領域記述情報により記述されるコードをコンテンツ中から抜き出し、前記コードから位置を示す情報を算出する手順を有するものである。

【００２２】

また、本発明（請求項１５）の暗号処理方法は、請求項１４記載の暗号処理方法であって、前記領域記述情報が２のべき乗で表現される単位長情報を含み、前記長さを示すコードに対して単位長情報のビットシフトを行う手順を有することを特徴とするものである。

【００２３】

また、本発明（請求項１６）の暗号処理方法は、請求項１４記載の暗号処理方法であって、暗号処理を開始する位置あるいは暗号処理を終了する位置を特定する手順を有するものである。

【００２４】

また、本発明（請求項１７）の暗号処理方法は、暗号処理を行う領域を記述する動作記述情報で特定された領域に暗号化あるいは復号化の暗号処理を行うことを特徴とする暗号処理方法であって、前記動作記述情報は、暗号化処理の方法を特定する情報を含む暗号記述情報を含み、暗号処理を行う領域を特定する情報を入力とし、前記暗号処理を行う領域に前記暗号記述情報で特定される暗号処理を施す手順を有するものである。

【００２５】

また、本発明（請求項１８）の暗号処理方法は、請求項１７記載の暗号処理方法であって、前記暗号記述情報が、基本暗号情報と一つ以上のオプション暗号情報から構成され、前記それぞれのオプション暗号情報は、オプションの暗号処理の方法を特定する情報と、前記オプションの適用される範囲を示す情報を含み、前記暗号処理を行う領域を基本暗号あるいはオプション暗号によって処理するかを前記範囲を示す情報から判定する手順を有することを特徴とするものである。

【００２６】

また、本発明（請求項１９）の暗号処理方法は、動作記述情報で特定された領域に暗号化あるいは復号化の暗号処理を行うことを特徴とする暗号処理方法において、前記動作記述情報は、コンテンツ中の同期情報の長さを示す情報と同期情報のパターンを示す情報を少なくとも持つ同期記述情報と、コンテンツ中の長さを示すコード位置を特定する情報と前記コードのビット長を特定する領域記述情報と、暗号化処理の方法を特定する情報を含む暗号記述情報を含み、前記同期記述情報により記述される同期情報をコンテンツから探索する手順と、前記領域記述情報により記述されるコードをコンテンツ中から抜き出し、前記コードから位置を示す情報を算出する手順と、暗号処理を行う領域を特定する情報を入力とし、前記暗号処理を行う領域に前記暗号記述情報で特定される暗号処理を施す手順とを有するものである。

【００２７】

また、本発明（請求項２０）の暗号処理方法は、請求項１９記載の暗号処理方法であって、前記位置を算出する手順を用いて、暗号処理を行う領域を検出するものである。

【００２８】

また、本発明（請求項２１）の暗号処理方法は、請求項１９記載の暗号処理方法であって、前記動作記述情報が命令の組み合わせであり、前記動作記述情報により記述される順番で、各手順の処理を行うものである。

【００２９】

また、本発明（請求項２２）の暗号処理方法は、請求項１９記載の暗号処理方法であって、前記動作記述情報が、前記同期記述情報、前記領域記述情報、前記暗号記述情報の組み合わせで構成されており、規定の順番で前記各手順を行うものである。

【００３０】

また、本発明（請求項２３）の記録媒体は、コンテンツ中の同期情報の長さを示す情報と同期情報のパターンを示す情報を少なくとも持つ同期記述情報と、コンテンツ中の長さを示すコード位置を特定する情報と前記コードのビット長を特定する領域記述情報と、暗号化処理の方法を特定する情報を含む暗号記述情報のうち少なくとも一つからなる動作記述情報を記録するものである。

【００３１】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照して説明する。

【００３２】

（実施の形態１）

実施の形態の説明に先立ち、実施の形態１で用いる用語について、簡単に説明を加える。

【００３３】

本実施の形態において、コンテンツとは、映像や音声やデータなどを含む任意のフォーマットのデジタル信号である。コンテンツの例としては、ＭＰＥＧ１の

映像あるいはＬａｙｅｒＩ、ＬａｙｅｒＩＩ、ＬａｙｅｒＩＩＩ（一般にＭＰ３と呼ばれている）の音声、ＭＰＥＧ２の映像あるいはＢＣ，ＡＡＣの音声、あるいはＴＳやＰＳなどのシステムストリーム、ＭＰＥＧ４の映像あるいはＡＡＣやＴｗｉｎＶＱなどの音声、あるいはシステムストリームがある。さらには、Ｄｏｌｂｙ－ＡＣ３の音声や、ＤＶフォーマットの映像や音声などがある。本実施の形態の暗号処理装置が取り扱うコンテンツはこれらの例に限られるものではなく、任意のフォーマットのコンテンツを処理の対象とすることができる。

【００３４】

また、本実施の形態において、暗号処理とは、暗号化処理あるいはその復号化処理を意味する。

【００３５】

また、動作記述情報については後程詳しく説明するが、暗号処理装置１の動作を制御するために、既定の文法によって記述されている可変長あるいは固定長の命令セット、あるいは既定の命令によって動作する場合には各命令において必要な制御情報のセットである。

【００３６】

（処理の概要）

以下、図１から図３を用いて、まずは本実施の形態の暗号処理装置の動作の概要を説明する。

【００３７】

図１は本発明の実施の形態１における暗号処理装置の構成図である。図１において、１１はプロセッサ、１２は同期検出部、１３は領域検出部、１４は暗号処理部、１５は入出力部、１６はレジスタである。

【００３８】

図２は、あるフォーマットのコンテンツに対する、本実施の形態の暗号処理装置１の動作例を説明する図である。コンテンツは、図２に示すように、既定の同期パターンに囲まれたパケット単位で処理が行われる。暗号処理装置１は動作記述情報に記述された同期パターンを検出し、その先頭ビットを開始位置とする。位置は、全てこの開始位置から何ビット目かで示される。次に、暗号処理装置１

は、動作記述情報に記述された動作により、終了位置を算出する。そして、終了位置に次の同期パターンが有るかどうかを検証する。また、暗号装置１は動作記述情報により記述された動作により、暗号開始位置および暗号終了位置を算出する。そして、暗号開始位置および暗号終了位置の間の領域を、暗号記述情報により記述された動作で暗号処理を行う。

【００３９】

以下の説明において、位置という言葉を用いる場合は、特に断りの無い限りは、開始位置（同期パターンの最初のビット）を０としたときに、何ビット目かを示すものとする。ただし、暗号開始位置は暗号処理を行う最初のビットであるが、暗号終了位置および終了位置はそれぞれ最終ビットの次の位置を示す。もちろん、これらに限られず、それぞれの実際の位置を特定可能な任意の表現方法を用いても良い。

【００４０】

図３は、上記の処理により検出・算出される情報の流れを、図１の構成図に重ねた説明図である。図３において、破線で示しているのがデータの流れである。これらの破線で示したデータのは、レジスタ１６を介して行われる方法、あるいは専用の信号線により各処理部など、任意の方法で交換することができる。

【００４１】

図３に示したように、同期検出部１２は同期パターンを検出し、同期パターンの開始位置を示す基本アドレスを出力する。また、終了位置に次の同期パターンが有るかどうかの検証を行う。領域検出部１３は、終了位置、暗号開始位置、暗号終了位置を算出する。暗号処理部１４は、暗号開始位置と暗号終了位置の間のデータを暗号処理する。　また、各処理の動作の内容や順番は、動作記述情報により記述されており、プロセッサ１１は、この動作記述情報に示されるように、各処理部の動作を制御する。各処理部（同期検出部１２、領域検出部１３、暗号処理部１４）も、動作記述情報によって記述された動作を行う。また、コンテンツは入出力部１５によって入出力される。また、データの流れについては、図３に示した装置間で行われるとは限られず、直接値が代入されるような構成でも良い。例えば、固定長のパケットの場合には、終了位置は固定値であるので、動作

記述情報によって記述された値がプロセッサによって直接代入される。以下の説明においては、レジスタを用いて交換するものとする。

【００４２】

次に、動作記述情報を記述するための、動作記述言語について説明する。基本となる動作記述言語の命令は、(表１)に示した4つの命令である。（表１）において、処理部はその命令により動作する処理部を、命令名は命令の名称を、動作は命令により行われる動作の名称を、記述情報は命令の引数として各処理部が必要とする記述情報を、それぞれ示す。

【００４３】

【表１】

処理部	命令名	動作	記述情報
同期検出部12	Sync_detect	同期検出動作	同期記述情報
	Sync_check	同期検証動作	
領域検出部13	Area_detect	領域検出動作	領域記述情報
暗号処理部14	Encrypt	暗号処理動作	暗号記述情報

暗号処理装置の基本命令

【００４４】

（表1）に示すように、基本となる命令は、Sync#detect，Sync#check，Area#detect，Encryptの４つの命令である。さらに、汎用命令として、レジスタに値を

セットするためのSet命令や、分岐を実現するためのLabel命令およびJump命令などを用いる。動作記述情報は、これらの命令の組み合わせにより暗号処理装置１の動作を制御を記述する情報である。動作記述言語の各命令は、可変長でも固定長でも良く、これらの命令を表現することができる任意の文法を選択可能である。暗号処理装置１の処理を軽減するためには、固定長のバイナリで表現されていることが望ましい。しかしながら、アスキーコードで表現された可変長の命令でも良い。この場合、プロセッサ１１あるいは、図１６に示したようなプロセッサの前段に設置された情報変換手段が、アセンブリ処理あるいはコンパイラ処理などを行い、固定長のバイナリの命令に変換しても良い。もちろん、各処理部が、アスキーコードや可変長コードを解釈するような構成にしても良いことは言うまでもない。

【００４５】

以下、上記の各命令による各処理部の動作をそれぞれ詳細に示す。

【００４６】

（同期検出部１２における同期検出動作）

最初に、Sync#detect命令による同期検出部１２の同期検証動作を説明する。

【００４７】

まず、命令について、詳細に説明する。同期検出命令は、

Sync#detect ＜終了位置＞　＜参照アドレス＞　＜同期記述情報＞

で表される。引数の＜終了位置＞および＜参照アドレス＞は、終了位置あるいは参照アドレスが格納されているレジスタに対応するアドレス、ＩＤ、変数名などである。参照アドレスは、コンテンツ中のどこから同期検出を開始するかを示すアドレス情報であり、通常は該コンテンツに始めてアクセスを開始する時にのみ参照される。また、引数の＜同期記述情報＞は、同期記述情報が格納されているレジスタに対応するアドレス、あるいは同期記述情報そのものである。同期パターンの長さを示す情報（sync#wide）および同期パターンを示す情報（sync#pattern）が少なくとも含まれている。sync#wideが0の時には、sync#patternは無くても良い。終了位置および参照アドレス、同期記述情報については、暗号処理装置１全体で既定の固定のレジスタを使用することにより引数から省くことが可能

である。

【００４８】

同期記述情報の表現形式は任意の形態を取ることが可能であるが、一例として、１ワード32bitsのレジスタに格納する時の例を図４に示す。ここで、sync#wideは8bits、sync#patternは32bitsとしており、図にしめしたように連続する２ワードのレジスタに格納される。＜同期記述情報＞がレジスタのアドレスを表す場合、ｎのアドレスを指定する。

【００４９】

同期検出動作では、コンテンツ中から動作記述情報で指示された同期パターンの検出を行う。検出が完了すると、他の処理部がコンテンツ中の同期パターンの開始位置を認識可能なように通知する。具体的には、同期の先頭ビットのアドレスを基本アドレスとして、各処理部が一意にアクセス可能なレジスタ（レジスタ名：Base#address）に格納する。以下の説明では、この方法により、基本アドレスを通知するものとする、しかしながら、開始位置の指示は、この方法に限定されず、専用線、専用レジスタなどを用いた任意の方法で他の処理部に基本アドレスを通知するような構成としても良い。さらに、基本アドレスにより通知する方法にも限定されない。例えば、コンテンツのパケットを処理するためのバッファに、パケット単位で読み込んでくる処理でも良い。あるいは、コンテンツがクロックとともに入力される場合には、コンテンツの同期パターンの先頭ビットが入力するタイミングでカウンタを０にする処理でも良い。以上に示したように、他の処理部が同期パターンの先頭ビットの場所が認識できる任意の処理を行えば良い。

【００５０】

図５は、同期検出部１２における、同期検出命令(Sync#detect)による同期検出動作のフローの例を示す図である。なお、同期検出処理は任意の処理フローにより実現可能であり、図５に示したフローに限定されるものではない。以下、図５のフロー例による同期検出動作について説明する。

【００５１】

まず、処理を開始すると（S1）、smodeの判定を行い（S2）、その結果によっ

て基本アドレスの値を設定する。smodeは、同期検出部１２の基本アドレスの生成方法を示す変数である。smode＝0の場合には、基本アドレスとして参照アドレスを設定する（S3）。また、smode＝１の場合には、基本アドレスとして、基本アドレスに終了位置を加算した値を設定する(S4)。また、smode＝２の場合には、基本アドレスはそのままにしておく。通常のsmodeの使われ方としては、初期化時すなわち、該コンテンツに初めてアクセスする時には０に設定されており、その後は１に設定される。また、エラー発生時の復帰処理などで同期検出命令の前に基本アドレスが設定されている場合には、２に設定される。smodeの使われ方はこれらに限定されず、基本アドレスの値の設定方法によって決められるべきである。

【００５２】

次にsync#wideの判定を行い（S5）、sync#wideが0の場合には、終了(S8)する。すなわち、現在の基本アドレスがそのまま基本アドレスとして有効とされる。

【００５３】

sync#wideが０でない場合には、同期探索（S6）を行う。同期探索(S6)では、コンテンツ上を、sync#wideで示されるビット数のウィンドウで、sync#patternと一致するパターンを、現在の基本アドレスからスタートして、1ビットずつシフトさせながら探していく処理を行う。例えば、sync#wide=12で、sync#pattern=0xFFFの場合、0xFFFに一致する最初のパターンを探す。一致するパターンが見つかると、同期パターンの先頭ビットを新しい基本アドレスとして設定する。もちろん、現在の基本アドレスで同期パターンと一致した場合には、現在の開始パターンをそのまま変更しない。同期探索(S6)の後、smodeを1に設定し(S7)、処理を終了(S8)する。

【００５４】

以上の処理により、同期記述情報によって記述された同期パターンを検出し、他の処理部に通知することが可能である。また、同期パターンを検出する必要の無い場合には、sync#wideを0に設定すれば良い。

【００５５】

（同期検出部１２における同期検証動作）

次に、Sync#check命令による同期検出部１２の同期検証動作を説明する。

【００５６】

まず、命令について、詳細に説明する。同期検証命令は、

Sync#check　＜終了位置＞　＜参照アドレス＞　＜同期記述情報＞

で表される。引数の＜終了位置＞および＜参照アドレス＞は、＜同期記述情報＞については、同期検出命令(Sync#derect)での記述と同じであるので、ここでは説明しない。

【００５７】

同期検証動作では、同期アドレスから終了位置だけ後ろ、すなわち同期アドレス＋終了位置のアドレスの位置に、同期記述情報で示される同期パターンがあるかどうかの検証を行う。ある場合には、ＴＲＵＥを意味する結果を返し、無い場合にはＦＡＬＳＥを意味する結果を返す。

【００５８】

図６は、同期検出部１２における、同期検証命令(Sync#check)による同期検証動作のフローの例を示す図である。なお、同期検出処理は任意の処理フローにより実現可能であり、図５に示したフローに限定されるものではない。以下、図５のフロー例による同期検出動作について説明する。

【００５９】

まず、処理を開始（S11）すると、sync#wideにより判定を行う。sync#wideが０の時には、TRUEを意味する結果を返し（S18）、終了(S19)する。

【００６０】

sync#wideが０より大きい場合には、同期チェックを行う(S13)。同期チェック(S13)はコンテンツの、基本アドレスから終了位置後、すなわち基本アドレス＋終了位置のデータが、同期記述情報で示される同期パターンと一致するかどうかチェックする。S13の処理の結果がNGすなわち一致しなかった場合と、OKすなわち一致した場合で処理が分岐される(S14)。OKの場合には、TRUEを意味する結果を返し(S18)、終了する（S19）。

【００６１】

同期チェックの結果がNGの場合には、smodeを2に設定し（S15）、エラー処理(

S16)を行う。この、S15とS16の処理については実装依存であり、必要であれば実行される。エラー処理（S16）では、二つの処理が実行される。一つは、他の処理部に対してエラーが発生したことを通知する処理である。これは、同期検証命令の結果が伝えられるならば、対応する必要がないが、そうでなければ対応が必要である。特に、他の処理部がパラレルに動作をしており、エラー時に何らかの処理を行わなければならない場合には、割り込みや専用線による通知が必要である。もう一つの処理は、エラー復帰のための処理である。具体的には、基本アドレスの値を変更する処理である。例えば、基本アドレスに１を加える方法（次の同期パターンを探索する）、基本アドレスに新しいアドレスを設定する方法などがある。

【００６２】

S15におけるsmode＝２の代入は、命令内部でエラー処理が行われたことを表現するために用いられるため、内部で処理が行われない場合には、S15の処理を行わない。

【００６３】

エラー復帰の処理については、ここ（S16）では何も行わず、Sync#checkの命令の外で、動作記述言語によって記述された命令セットにより実現することもできる。すなわち、動作記述情報中に動作として記述することもできる。この場合、結果がFALSEであり、かつ、smodeが２以外の場合の処理として、基本アドレスへの値の代入や値の加算などの演算処理や、smodeへの値の代入などの組み合わせによって記述すれば良い。

【００６４】

S15およびS16の処理の後に、FALSEを意味する結果を返し（S17）、処理を終了する（S19）。

【００６５】

以上の処理により、基本アドレスから終了位置後に正しい同期パターンが有るかどうかの検証を行う事ができる。

【００６６】

（領域検出部１３における領域検証動作）

次に、Area#detect命令による領域検出部１３の領域検証動作を説明する。

【００６７】

まず、命令について、詳細に説明する。領域検証命令は、

Area#detect ＜位置＞　＜領域記述情報＞

で表される。引数の＜位置＞は、領域検出処理を行った結果の位置が格納されるレジスタに対応するアドレス、ＩＤ、変数名などである。引数の＜領域記述情報＞は、領域記述情報が格納されているレジスタに対応するアドレス、あるいは領域記述情報そのものである。

【００６８】

領域記述情報には、コンテンツ中に埋め込まれている長さ情報（length#code）に関する情報として、基本アドレスからの位置を示す情報(length#pnt)、length#code自身の長さを示す情報(length#wide)、length#codeの単位長さを示す情報(length#unit)、length#codeの形式を示す情報(length#type)が含まれている。length#wideが0の時には、他の情報は無くても良い。length#unitは、length#codeの単位が何であるかを示すための情報である。その表現形式は任意であるが、ほとんどの場合は、1bit、8bits、32bitsなどで表されると考えられるので、2のべき乗で表現する。すなわち、length#codeで表されるbit長は、length#code×(2**length#unit)となる。２のべき乗で表現することにより、掛け算がビットシフトのみで実現可能なので、装置構成を簡単にできるという効果がある。もちろん、これに限定されるものではなく、単純にlength#unitで何倍かを表し、掛け算するような構成としても良い。また、length#typeは、符号付きか符号無しか、MSBファーストかLSBファーストかを示す情報である。

【００６９】

また、領域記述情報には、コンテンツ中に埋め込まれているフラグ情報(flag#code)に関する情報として、基本アドレスからの位置を示す情報(flag#pnt)、flag#codeの長さを示す情報(flag#wide)、flag#codeのパターンを示す情報(flag#pattern1, flag#pattern2)を含む。flag#wideが０の時には、他の情報はなくても良い。flag#pattern1およびflag#pattern2は、一致パターンであり、二つある必要はなく、少なくとも一つで良い。

【００７０】

また、領域記述情報には、オフセット情報（offset）が含まれている。offset情報は、符号付きの整数で表現された数値である。

【００７１】

また、領域記述情報には、加算するか代入するかのフラグ（as）が含まれている。asが0の時、計算結果の長さが位置に加算され、1の時は、位置に代入される。

【００７２】

以上示した領域記述情報の表現形式は任意の形態を取ることが可能であるが、一例として、１ワード32bitsのレジスタに格納する時の例を図７に示す。ここで、asは1bit、flag#wideは3bits、flag#pattern1およびflag#pattern2はそれぞれ4bits、flag#pntは16bits、offsetは32bits、length#wideは8bits、length#typeは2bits、length#unitは3bits、length#pntは16bitsとしており、図にしめしたように連続する３ワードのレジスタに格納される。＜領域記述情報＞がレジスタのアドレスを表す場合、ｎのアドレスを指定する。

【００７３】

領域検出動作では、flag#pntおよびflag#wideの指示によりコンテンツから抜き出したflag#codeが、flag#pattern1あるいはflag#pattern2に一致する時に、length#pntおよびlength#wide、length#typeの指示により抜き出したlength#codeに２のlength#unit乗を掛けた値と、offsetとの加算結果を、算出結果とする。さらに、該算出結果をasの指示によって、位置に加算あるいは代入する処理を行う。flag#codeおよびlength#codeの抜き出しについては、図９に示す。＊#wideと＊#pntの指定によって、同期ビットの先頭から＊#pntビット後から、＊#wideビット分のデータを抜き出し、＊#codeとする。

【００７４】

図８は、領域検出部１３における、領域検証命令(Area#check)による領域検証動作のフローの例を示す図である。なお、領域検出処理は任意の処理フローにより実現可能であり、図５に示したフローに限定されるものではない。以下、図５のフロー例による領域検出動作について説明する。

【００７５】

まず、処理を開始（S21）すると、flag#wideにより判定を行う。flag#wideが０の時には、s26へ飛ぶ。flag#wideが０より大きい時には、S23からS25のflag判定処理を行う。

【００７６】

まず、コンテンツからflag#pnt、flag#wideで示されるflag#codeを読み出す（S23）。読み出したflag#codeを判定する（S24）。flag#codeとflag#pattern1およびflag#pattern2の双方と比較を行い、いずれか一方でも一致すれば、結果を１とし、一致しない場合は結果を０とする。結果の判定を行い（S25）、一致しない場合には、位置への加算や代入を行わず終了（S33）する。一致した場合には、S26の処理へ移る。

【００７７】

flag#wideが0あるいは、flag#codeの判定結果が一致した場合、length#wideの判定を行う(S26)。length#wideが0の場合には、length#codeを0とし(S27)、0以上の場合には、length#pnt、length#wideで示されるlength#codeを読みだす(S28)。次に、lengthの算出を行う(S29)。lengthの算出は、length#code×（２のlength#unit乗）＋offsetで求められる。ここで、length#codeはlength#typeの情報を元に型変換された後に演算される。次に、asの判定を行う（S30）。asが0の場合には、位置にlengthが加算され(S31)、1の場合には代入される(S32)。その後処理が終了する(S33)。

【００７８】

以上の処理により、領域記述情報で記述された方法により、コンテンツから情報を抜きだし、領域記述情報で記述された方法により、長さを算出し、位置のレジスタに設定できる。この命令を用いることにより、コンテンツ中の長さ情報あるいは／およびフラグ情報、および／あるいは固定値を用いて算出可能な、任意の位置の計算を指示できる。もし、コンテンツ中に長さ情報が二つある場合など、一回の命令で算出できない場合には、本命令を2回繰り返すことで算出可能である。

【００７９】

なお、領域検出動作を指示する命令については、上記説明した領域検出命令に限られるものではなく、上記の領域検出命令を複数の命令で実現しても良い。例えば、フラグに関する領域記述情報からflag#codeを検出して照合する命令と、長さに関する領域記述情報からlength#codeを検出してlengthを算出するような命令を組み合わせて実現しても良い。あるいは、コンテンツ中のコードの位置（pnt）とコードの長さ（wide）を示す記述情報を入力し、該記述情報で示されるコードをコンテンツから抜き出す命令と、加算を行う命令、ビットシフトを行う命令、比較を行う命令、などを組み合わせることにより実現しても良い。これらのように、命令を分割することにより、一つのArea#detect命令で算出できないような領域の計算を、より効率的に実現可能である。あるいは、一部の処理のみ必要な場合に、動作を効率化することが可能である。しかしながら、Area#detect命令を用いた場合には、ほとんどの既存のフォーマットに対しては、Area#detect命令のみで対応可能であるので、動作記述情報の構成が容易である。もちろん、Area#detect命令および、その分割した場合の命令の全てを使用可能とし、動作記述情報を構築する場合にこれらを組み合わせることによって、より効率的に動作記述情報を生成できる。

【００８０】

なお、領域検出動作を指示する命令については、上記説明した命令に限られるものではない。テーブル設定とテーブル参照のための命令を用意することにより、より複雑な計算を実現できる。例えば、コンテンツ中のコードとパケット長の対応が式であらわせない場合、複雑な処理の場合には、テーブル設定とテーブル参照を用いれば、容易に動作の記述が可能となる。

【００８１】

（暗号処理部１４における暗号処理動作）

次に、Encrypt命令による暗号処理部１４の暗号処理動作を説明する。

【００８２】

まず、命令について、詳細に説明する。暗号処理命令は、

Encrypt ＜暗号開始位置＞ ＜暗号終了位置＞ ＜暗号記述情報＞

で表される。引数の＜暗号開始位置＞および＜暗号終了位置＞は、暗号開始位置

および暗号終了位置が格納されているレジスタに対応するアドレス、ＩＤ、変数名などである。引数の＜暗号記述情報＞は、暗号記述情報が格納されているレジスタに対応するアドレス、あるいは暗号記述情報そのものである。暗号開始位置および暗号終了位置、暗号記述情報については、暗号処理装置１全体で既定の固定のレジスタを使用することにより引数から省くことも可能である。

【００８３】

暗号記述情報には、少なくとも、暗号化を行うか復号化を行うかを示すフラグ(ed)が含まれている。edが0の時、暗号化処理を行い、1の時には復号化処理を行う。

【００８４】

また、暗号記述情報には、少なくとも、基本暗号アルゴリズムのアルゴリズム番号（Cipher#algorithm[0]）、暗号処理モード（Cipher#mode[0]）、ブロック長（Cipher#block[0]）が含まれている。Cipher#algorithmは、使用する暗号アルゴリズムを指示する番号である。例えば、DESやFEALやRSAなどのアルゴリズムに対応する番号が決められおり、その番号を指示する。また、Cipher#modeは使用する暗号モードを指示する番号である。例えば、ECBモードや、CBCモード、OFBモードに対応する番号が決められており、その番号を指示する。また、Cipher#blockは使用する暗号のブロック長を指示する。

【００８５】

また、暗号記述情報には、オプションを何個使用するかを指示するオプション番号(no)が含まれている。さらに、オプション番号で指示される数のオプションが含まれる。オプションは、オプションが適用される境界の方向を示すフラグ(bd[n])、オプションが適用される境界の長さを指示する(boundary[n])、オプションの暗号アルゴリズム番号(Cipher#algorithm[n])、暗号処理モード(Cipher#mode[n])、ブロック長(Cipher#block[n])がそれぞれ含まれている。Cipher#algorithm[n]、Cipher#mode[n]、Cipher#block[n]については、基本暗号と同じである。bd[n]が0の時、そのオプションは前から、すなわち暗号開始位置からboundary[n]後ろまで適用される。bd[n]が１の時、そのオプションは後ろから、すなわち、暗号終了位置からboundary[n]前まで適用される。

【００８６】

以上示した領域記述情報の表現形式は任意の形態を取ることが可能であるが、一例として、１ワード32bitsのレジスタに格納する時の例を図１０に示す。ここで、edは1bit、noは3bits、Cipher#algorithm[0]は8bits、Cipher#mode[0]は8bits、Cipher#block[0]は8bits、また、オプションとして、bd[n]は1bis、baundary[1]は16bits、Next#IDは8bits、Cipher#algorithm[1]は8bits、Cipher#mode[1]は8bits、Cipher#block[1]は8bitsとしており、図に示したように連続する３ワードのレジスタに格納される。＜暗号記述情報＞がレジスタのアドレスを表す場合、ｎのアドレスを指定する。さらに、オプションが二つ以上ある場合には、Next#IDにより、オプションが格納されているレジスタのアドレスを指示する。次のオプションは、Next#IDから連続する２ワードのレジスタに格納される。

【００８７】

暗号処理動作では、暗号開始位置と暗号終了位置の間の領域に対して、暗号記述情報で示される暗号処理を行う。図１１に暗号処理の概要を示す。

【００８８】

各領域にどの暗号処理が適用されるかは、オプションは番号が小さいほど優先され、基本暗号は最も優先度が少ない。すなわち、各オプションの暗号処理は、bd[n]およびbaundary[n]で指示される領域に適用されるが、重なった場合には、オプションの番号ｎが小さいほうの処理が優先される。基本暗号は、オプションによって指示されていない領域に適用される。図１１の例で言うと、オプション１で指示される境界領域が１２８、オプション２で指示される境界領域が１２６、オプション３で指示される境界領域が１２７である。この場合、オプション２と３の境界領域に重なりができるが、ｎが小さいオプション（２）が優先され、１２１の領域がオプション（２）で処理され、１２２の領域がオプション（３）で処理される。残った１２３の期間は基本暗号で処理される。また、各領域の処理は、暗号化のブロック単位で判定され、ブロックの先頭が属している領域の処理に従う。すなわち、ブロック１３０、１３１は基本暗号で処理され、ブロック１３２、１３３はオプション（１）で処理される。

【００８９】

図１２は、暗号処理部１４における、暗号処理命令(Encrypt)による暗号処理動作のフローの例を示す図である。なお、暗号処理動作は任意の処理フローにより実現可能であり、図１２に示したフローに限定されるものではない。以下、図１２のフロー例による暗号処理動作について説明する。

【００９０】

まず、処理を開始（S40）すると、現在位置を示す内部変数pntに暗号開始位置を代入する(S41)。次に、基本暗号あるいはどのオプション暗号で処理を行うかの暗号の選択処理によりｎが決定される。(S42)。暗号の選択(S42)のフロー例は、図１３に示されている。以下、図１３を用いて暗号の選択処理の動作を説明する。

【００９１】

処理を開始(S51)後、ｎを0に設定する(S52)。次に、ｎに１を加算する(S53)。その後、ｎとonを比較（S54）し、onの方が大きければ、基本暗号を使用するので、nを０にして（S60）終了する(S61)。S54の比較結果が、同じかonが大きければ、オプション(n)の判定に移り、まずbd[n]の値を判定する(S55)。

【００９２】

bd[n]が0の場合、境界位置として暗号開始位置にbaoundary[n]を加算（S56）し、pntすなわち現在位置と比較する（S57）。比較結果が同じかpntが大きかった場合、オプション（ｎ）の領域に含まれていないので、再びS53へジャンプし、次のオプションの判定に移る。S57の比較結果がpntが小さかった場合には、そのオプション（ｎ）の領域に含まれているので、そのまま終了（S61）する。

【００９３】

S55での比較結果がbd[n]が1の場合、境界位置として暗号終了位置からbaoundary[n]を減算（S58）し、pntすなわち現在位置と比較する（S59）。比較結果がpntが小さかった場合、オプション（ｎ）の領域に含まれていないので、再びS53へジャンプし、次のオプションの判定に移る。S59の比較結果が同じか、pntが大きかった場合には、そのオプション（ｎ）の領域に含まれているので、そのまま終了（S61）する。

【００９４】

上記の暗号選択処理(S41)により、ｎが決定される。その後、edの判定（S43）が行われる。edが0の場合、Cipher#block[n]ビットのブロックを、Cipher#algorithm[n]の暗号を用いてCipher#mode[n]の暗号モードで暗号化処理(S44)する。edが1の場合、Cipher#block[n]ビットのブロックを、Cipher#algorithm[n]の暗号を用いてCipher#mode[n]の暗号モードで復号化処理(S45)する。

【００９５】

S44あるいはS45の処理後、次の暗号ブロックの処理に移るため、pntにCipher#block[n]を加算する(S46)。次に、pntと暗号終了位置の比較を行い（S47）、同じかpntが大きければ、暗号開始位置と暗号終了位置の間の領域についてはすべて処理が終わったので、終了する(S48)。S47の比較の結果、pntが小さければ、まだ処理する領域が残っているので、再びS42の処理に戻る。

【００９６】

以上の処理により、暗号記述情報で記述された方法により、暗号開始位置と暗号終了位置の間の領域のコンテンツを、暗号処理できる。

【００９７】

なお、暗号処理命令の構成や動作については、上記の例に限られるものではない。例えば、コンテンツ中に埋め込まれたコードが、指示したパターンに一致する場合にのみ暗号処理を行うような構成にしても良い。この場合、領域検出命令におけるフラグ照合で用いるのと同様の記述情報を用いて、同様の動作によって実現できる。これを用いれば、パケットを識別する識別子が、記述情報で記述したパターンに一致したときにのみ暗号処理を行うような構成にすることが可能である。さらにこの命令を用いれば、複数の命令を用いることにより、識別子毎に異なる暗号処理を行うことも可能である。また、領域記述情報に鍵ファイルへアクセスするための情報（アドレス情報など）を含むことにより、鍵ファイルと対応させて動作を制御することも可能である。

【００９８】

なお、暗号処理命令の構成や動作については、上記の例に限られるものではない。オプションの数（on）については、少なくても１以上であれば、任意の数範囲としても良い。

【００９９】

（全体の処理の流れ）

次に、図１４に動作記述情報により指示される動作の流れの具体的な例を示す。処理が開始される（Ｓ１０１）と、まず同期検出部１２によって同期パターンの検出動作、すなわちＳｙｎｃ＿ｄｅｔｅｃｔ命令による動作が行われる（Ｓ１０２）。これにより、基本アドレスが求められる。同期検出が終わると、領域検出部１３において、終了位置の検出がＡｒｅａ＿ｄｅｔｅｃｔによって行われれる（Ｓ１０３）。これは、コンテンツ中から抜き出された長さ情報や、既定の値から求められる。次に、再び同期検出部１２において、終了位置に正しい同期パターンがあるかどうかの同期検証（Ｓｙｎｃ＿ｃｈｅｃｋ）が行われる（Ｓ１０４）。結果がＮＧ（Ｓ１０５）、すなわち終了位置で示される位置に正しい同期パターンが無かった場合には、再びＳ１０１で処理を開始する。結果がＯＫ（Ｓ１０５）の場合には、領域検出部１３において、暗号開始位置および暗号終了位置の検出を行う（それぞれ、Ｓ１０６とＳ１０７）。最後に、暗号処理部１４において、暗号開始位置と暗号終了位置の間を暗号処理する（Ｓ１０８）。

【０１００】

以上の処理を行うように、動作記述言語の命令をならべたものを、動作記述情報とすれば良い。これにより、動作記述情報の指示によりコンテンツ中の暗号処理を行う領域を決定し、その領域に動作記述情報で指示された暗号処理を行うことが可能である。

【０１０１】

なお、動作記述情報における命令の組合わせは、図１４に示したものに限られるものではない。例えば、暗号開始位置の検出（Ｓ１０６）については、Area#detectを用いず、固定の値を暗号開始位置に設定するような構成でも良い。また、同期検証（sync#check）の処理を、暗号処理が終わった後に行っても良い。クロックに同期したコンテンツが入力される場合には、この方法で同期の検証を行う。動作記述情報における命令の組合わせは、そのコンテンツのフォーマットや適用する暗号処理方法に応じて、自由に設定可能である。

【０１０２】

なお、暗号記述情報については、上記示したような命令の組合わせとしたが、これに限られない。例えば、固定的に図１４の処理を行うような構成とし、暗号記述情報としては、各命令において使用する同期記述情報、領域記述情報、暗号記述情報を用いるような構成としても良い。この場合、領域記述情報としては、終了位置、暗号開始位置、暗号終了位置のそれぞれに対応する情報が必要である。これによれば、拡張性は失われるが、容易に動作記述情報を構成可能であり、ほとんどのコンテンツフォーマットに対しては適用可能である。あるいは、拡張性を保つために、上記の各記述情報を設定し、図１４に示すような動作を１命令で行うような命令を用意しても良い。

【０１０３】

なお、本発明の実施の形態の暗号処理装置は、図１に示した構成としたが、これにかぎられない。暗号開始位置や暗号終了位置が固定値、あるいは他の装置から情報として供給されるば場合には、同期検出部１２および領域検出部１３が不要となる。より簡単な構成で、暗号処理を実現可能である。

【０１０４】

なお、本発明の実施の形態の暗号処理装置は、図１に示した構成としたが、これにかぎられない。例えば、同期処理部１２、領域処理部１３、暗号処理部１４の処理をプロセッサ１１の処理として実現するような形態でも良い。

【０１０５】

なお、本発明の動作記述情報の伝送方法については特に示さなかったが、該コンテンツとの関連を示しさえすれば、任意の方法で伝送可能である。例えば、コンテンツとともに記録媒体に記録されていても良いし、コンテンツとともに伝走路を伝送されても良い。さらに、パケット毎に異なる暗号処理命令を、パケットと対応させて、伝送あるいは記録する方法を用いても良い。

【０１０６】

なお、本発明の実施の形態1の暗号処理装置は、暗号化装置としてもその復号化装置としても使用可能である。もちろん、暗号化の機能のみを具備した暗号化装置、あるいは復号化装置の機能のみを具備した復号化装置とすることもできる。また、本実施の形態の暗号処理装置を用いて、暗号化した後のコンテンツと動

作記述言語を別々に、あるいは多重して伝送路に暗号化して送信する暗号化送信装置、あるいは受信して復号化するような復号化受信装置に用いることもできる。さらに、暗号化した後のコンテンツと動作記述言語を別々に、あるいは多重して記録する暗号化記録装置、あるいは再生して復号化するような復号化再生装置を構成することもできる。

【０１０７】

なお、本発明の実施の形態1では、主にコンテンツをメモリから読み出すような構成とし、同期検出部１２が検出した同期パターンの位置を示す基本アドレスを設定するような構成としているが、これに限られるものではない。例えば、コンテンツがクロックに同期あるいはバースト的に入力されるような構成としても良い。この場合には、コンテンツの一部が遅延装置に蓄積され、同期検出部１２はその遅延装置中のどの位置が同期パターンか他の処理部が認識可能な任意の方法で処理を行う。例えば、遅延装置の先頭が同期パターンの先頭となるように遅延装置からデータを読み出す方法や、ビット位置を示すカウンタの値を、同期パターンを検出した時に０にするような方法がある。

【０１０８】

なお、本発明の実施の形態1の暗号処理装置においては、上記で説明したような同期検出部１２、領域検出部１３、暗号処理部１４を具備するような構成としたが、これに限られるものではない。動作記述情報によって動作する同期検出部１２のみを具備し、他の処理部は固定的に処理するような構成あるいは、無くても良い。これによれば、動作記述情報で同期検出を制御可能な装置を構成可能であるという効果が得られる。これは、動作記述情報によって動作する領域検出部１３のみ具備する、あるいは暗号処理部１４についても同様であり、それぞれ、動作記述情報により領域の検出を制御可能、動作記述情報により暗号処理を制御可能という効果が得られる。また、いずれか二つの組合わせによっても同様に効果を得ることができる。

【０１０９】

また、同期検出部１２および領域検出部１３のいずれか、あるいは両方の組み合わせについては、暗号処理装置での使用に限定されず、暗号以外の任意の処理

に適用することができる。すなわち、指定された領域に信号処理を行うような処理部を暗号処理部１４の代わりに用いることにより、コンテンツのある特定の部分にのみ処理したいような任意の処理に適用できる。

【０１１０】

なお、本発明の実施の形態１の暗号処理装置においては、領域検出部１３が一つ有るような構成としたが、これに限られない。領域検出部１３が複数有っても良い。この場合、動作記述情報に複数の領域検出命令がある場合に、複数の領域検出命令を異なる領域検出部１３で別々に処理しても良い。例えば、３つの領域検出部１３を持ち、それぞれで終了位置、暗号開始位置、暗号終了位置を検出するような構成としても良い。これによれば、領域検出命令による処理を並列に処理できるので、処理時間の短縮を図ることができる。命令の振り分けは、プロセッサ１１が行っても良いし、それぞれの領域検出部１３に異なる命令を割り当てることによって実現しても良い。

【０１１１】

【発明の効果】

以上のように本発明（請求項１）の暗号処理装置および、本発明（請求項１２）の暗号処理方法によれば、任意のフォーマットのコンテンツに対して、動作記述情報によってコンテンツ中の同期信号の検出を制御可能である。

【０１１２】

また、以上のように本発明（請求項２）の暗号処理装置および、本発明（請求項１３）の暗号処理方法によれば、任意のフォーマットのコンテンツに対して、動作記述情報によってコンテンツ中の同期信号を検出および検証を制御可能であり、同期信号の御検出を防止できる。

【０１１３】

また、以上のように本発明（請求項３）の暗号処理装置および、本発明（請求項１４）の暗号処理方法によれば、任意のフォーマットのコンテンツに対して、動作記述情報によってコンテンツ中の任意の長さ情報の抜き出しと算出が可能である。

【０１１４】

また、以上のように本発明（請求項４）の暗号処理装置および、本発明（請求項１５）の暗号処理方法によれば、任意のフォーマットのコンテンツに対して、簡単な構成により、長さ情報の算出が可能である。

【０１１５】

また、以上のように本発明（請求項５）の暗号処理装置および、本発明（請求項１６）の暗号処理方法によれば、任意のフォーマットのコンテンツに対して、動作記述情報によって、暗号処理の開始あるいは終了位置を検出可能である。

【０１１６】

また、以上のように本発明（請求項６）の暗号処理装置および、本発明（請求項１７）の暗号処理方法によれば、動作記述情報によって、任意の暗号処理方法を制御可能である。

【０１１７】

また、以上のように本発明（請求項７）の暗号処理装置および、本発明（請求項１８）の暗号処理方法によれば、任意のフォーマットのコンテンツに対して、動作記述情報によって、一つのパケットに対する複数の暗号処理の適用を制御可能である。

【０１１８】

また、以上のように本発明（請求項８、９）の暗号処理装置および、本発明（請求項１９、２０）の暗号処理方法によれば、任意のフォーマットのコンテンツに対して、動作記述情報によって、同期位置の検出、暗号化する領域の検出、および暗号化処理の制御を可能にする。

【０１１９】

また、以上のように本発明（請求項１０）の暗号処理装置および、本発明（請求項２１）の暗号処理方法によれば、動作記述情報によって、処理の回数や順番を制御できるので、任意のフォーマットに対して暗号化処理の制御を可能とする。

【０１２０】

また、以上のように本発明（請求項１１）の暗号処理装置および、本発明（請求項２２）の暗号処理方法によれば、ユーザが動作記述情報を容易に生成可能で

ある。

【０１２１】

また、以上のように本発明（請求項２３）の記録媒体によれば、暗号処理装置を制御可能な情報を記録できる。

【図面の簡単な説明】

【図１】

本発明の第1の実施の形態の暗号処理装置の構成を示す図

【図２】

本発明の第１の実施の形態の暗号処理装置の動作を説明する図

【図３】

本発明の第１の実施の形態の暗号処理装置の動作例を示す図

【図４】

本発明の第１の実施の形態の暗号処理装置の動作フローの例を示す図

【図５】

本発明の第１の実施の形態の暗号処理装置における同期検出部に関する動作記述情報を示す図

【図６】

本発明の第１の実施の形態の暗号処理装置における同期検出部の動作フローを示す図

【図７】

本発明の第１の実施の形態の暗号処理装置における同期検出部の動作フローを示す図

【図８】

本発明の第１の実施の形態の暗号処理装置における領域検出部に関する動作記述情報を示す図

【図９】

本発明の第１の実施の形態の暗号処理装置における領域検出部の動作フローを示す図

【図１０】

本発明の第１の実施の形態の暗号処理装置における領域検出部の動作を説明する図

【図１１】

本発明の第１の実施の形態の暗号処理装置における暗号処理部に関する動作記述情報を示す図

【図１２】

本発明の第１の実施の形態の暗号処理装置における暗号処理部の動作を説明する図

【図１３】

本発明の第１の実施の形態の暗号処理装置における暗号処理部の動作フローを示す図

【図１４】

本発明の第１の実施の形態の暗号処理装置における暗号処理部の動作フローを示す図

【図１５】

本発明の第１の実施の形態の暗号処理装置における暗号処理部の別の構成を示す図

【図１６】

従来の暗号処理装置の動作を説明する図

【符号の説明】

１　暗号処理装置

１１　プロセッサ

１２　同期検出部

１３　領域検出部

１４　暗号処理部

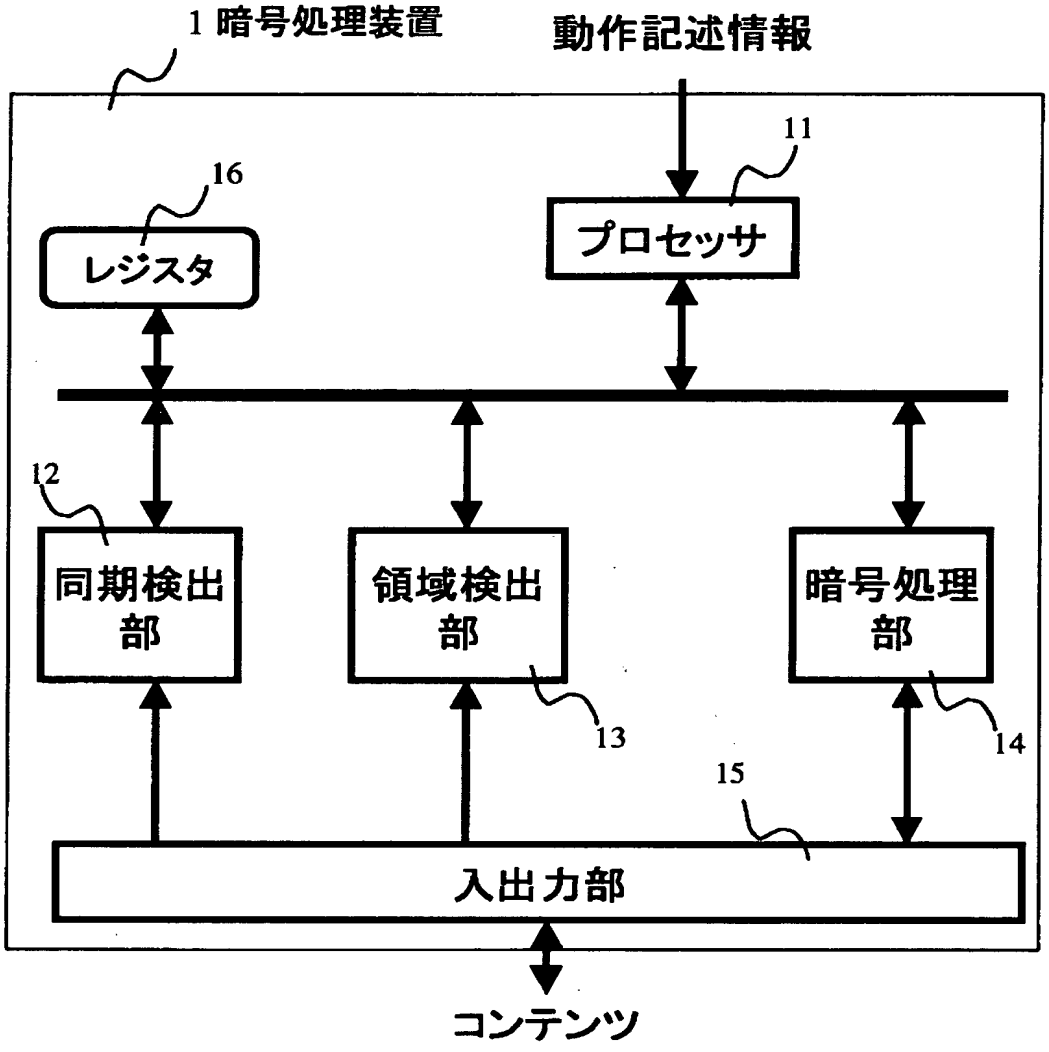
１５　入出力部

１６　レジスタ

１７　情報変換手段

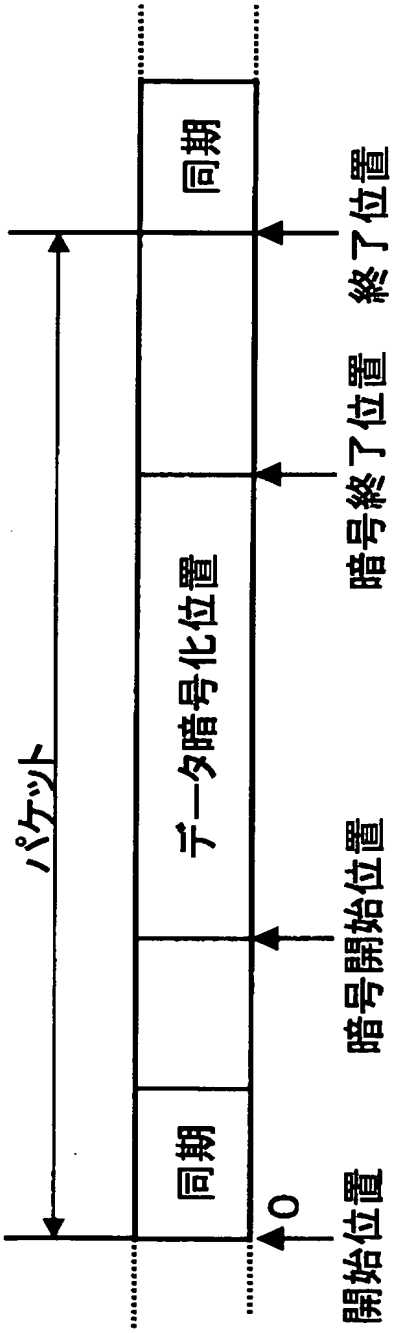
【書類名】　図面

【図１】

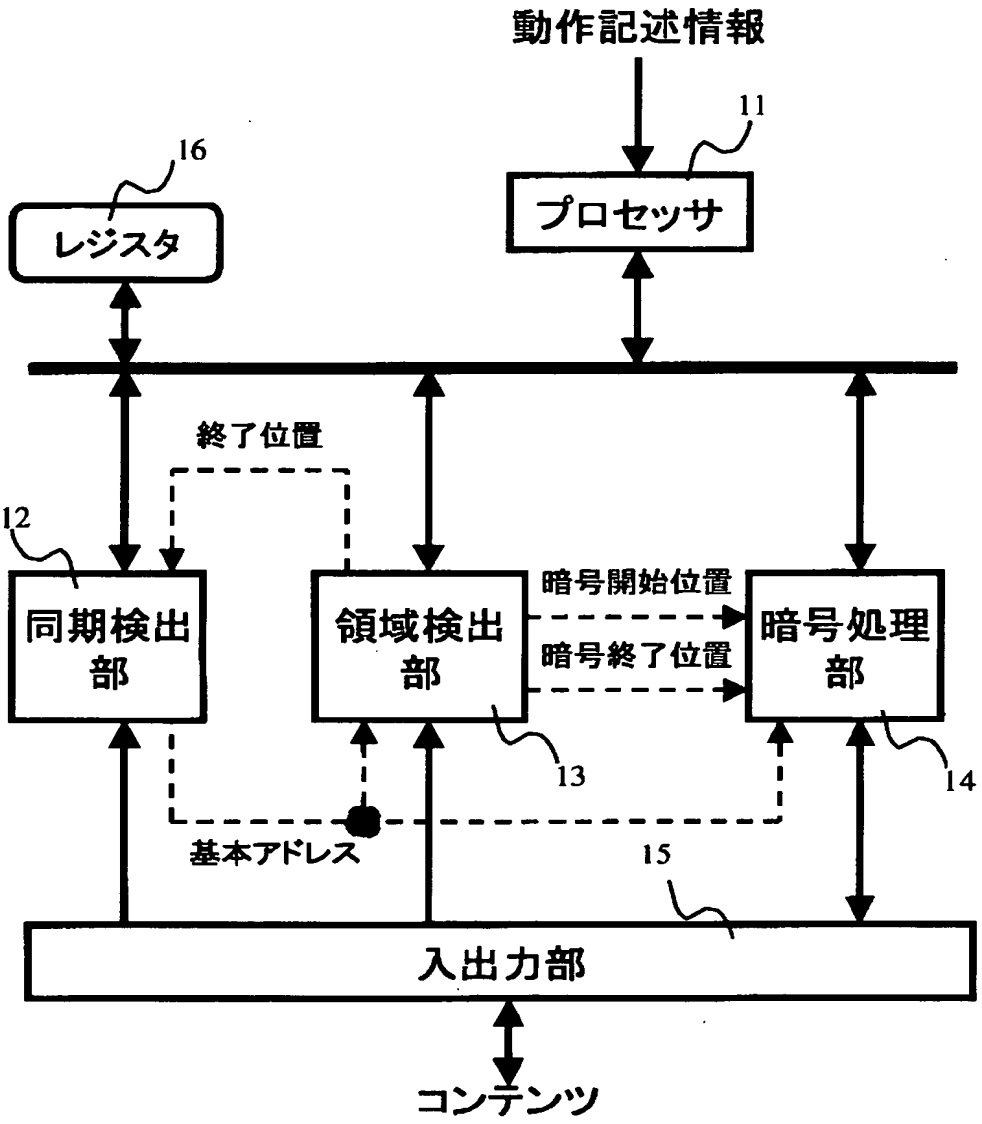


出証特２０００－３０４１２２３

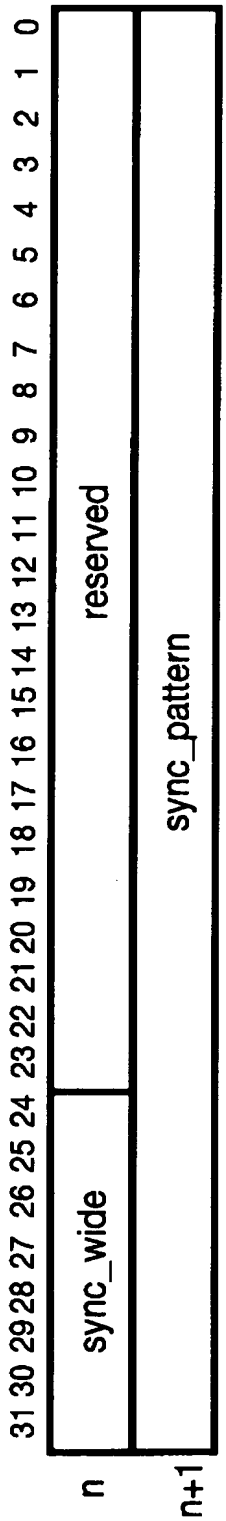
【図２】



【図３】

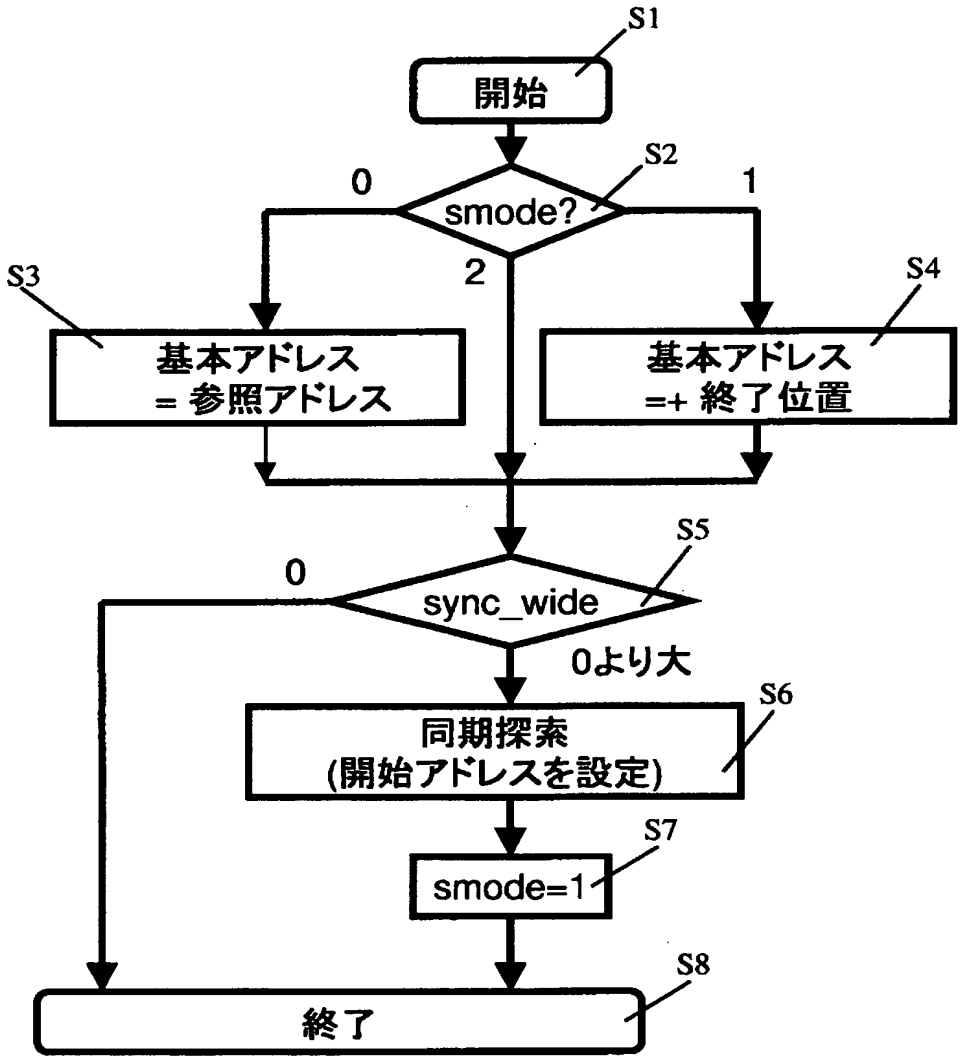

動作記述情報
11
16
プロセッサ
レジスタ
終了位置
12
同期検出部
領域検出部
暗号開始位置
暗号終了位置
暗号処理部
13
14
基本アドレス
15
入出力部
コンテンツ

【図４】


31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
sync_wide
reserved
sync_pattern
n
n+1

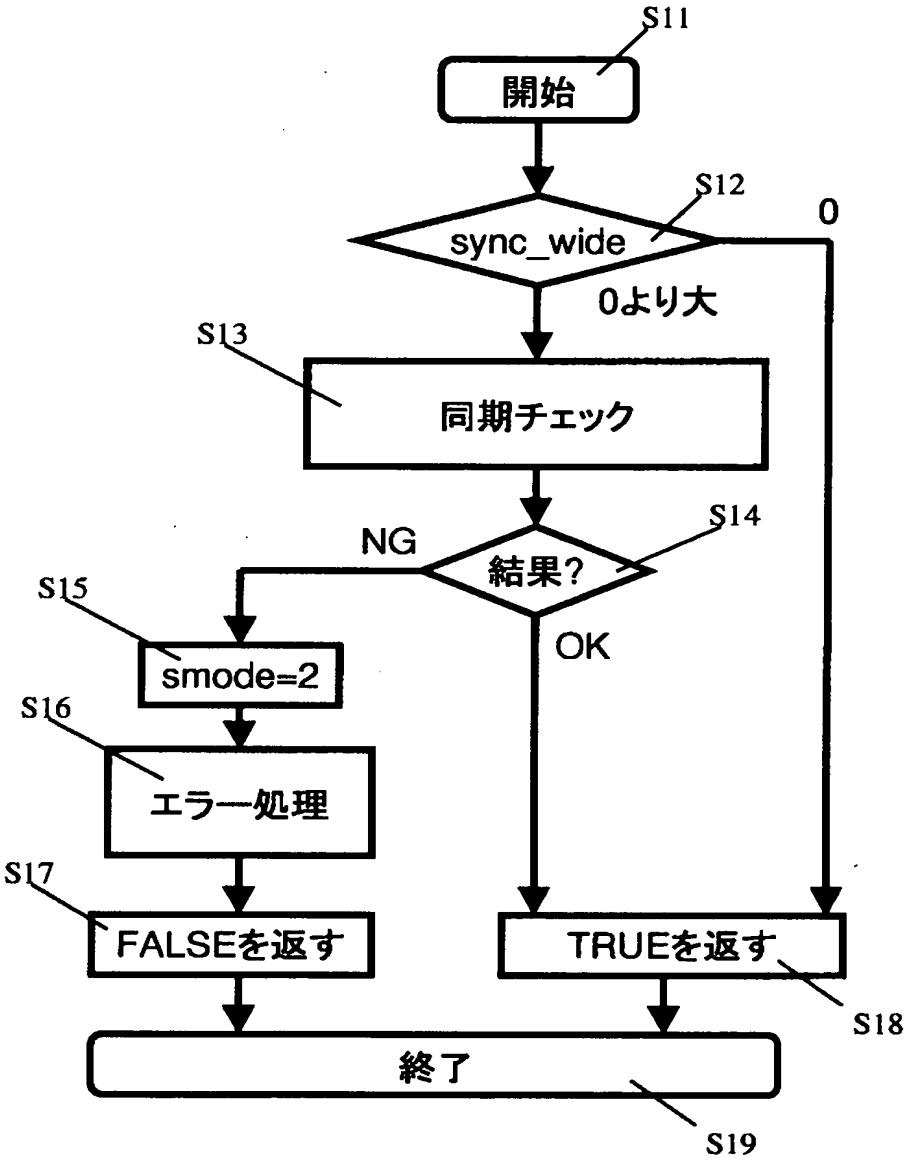
【図５】

同期検出命令

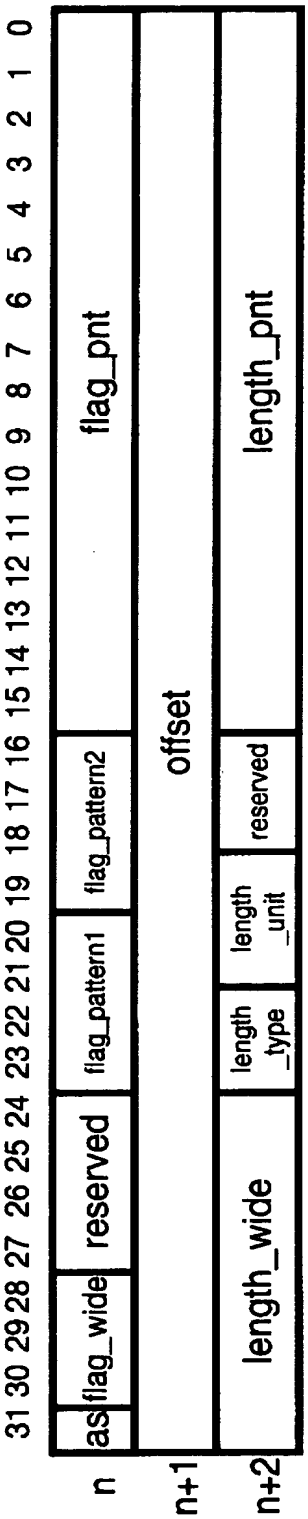

S1
開始
S2
smode?
0
1
2
S3
基本アドレス
= 参照アドレス
S4
基本アドレス
=+ 終了位置
S5
sync_wide
0
0より大
S6
同期探索
(開始アドレスを設定)
S7
smode=1
S8
終了

【図６】

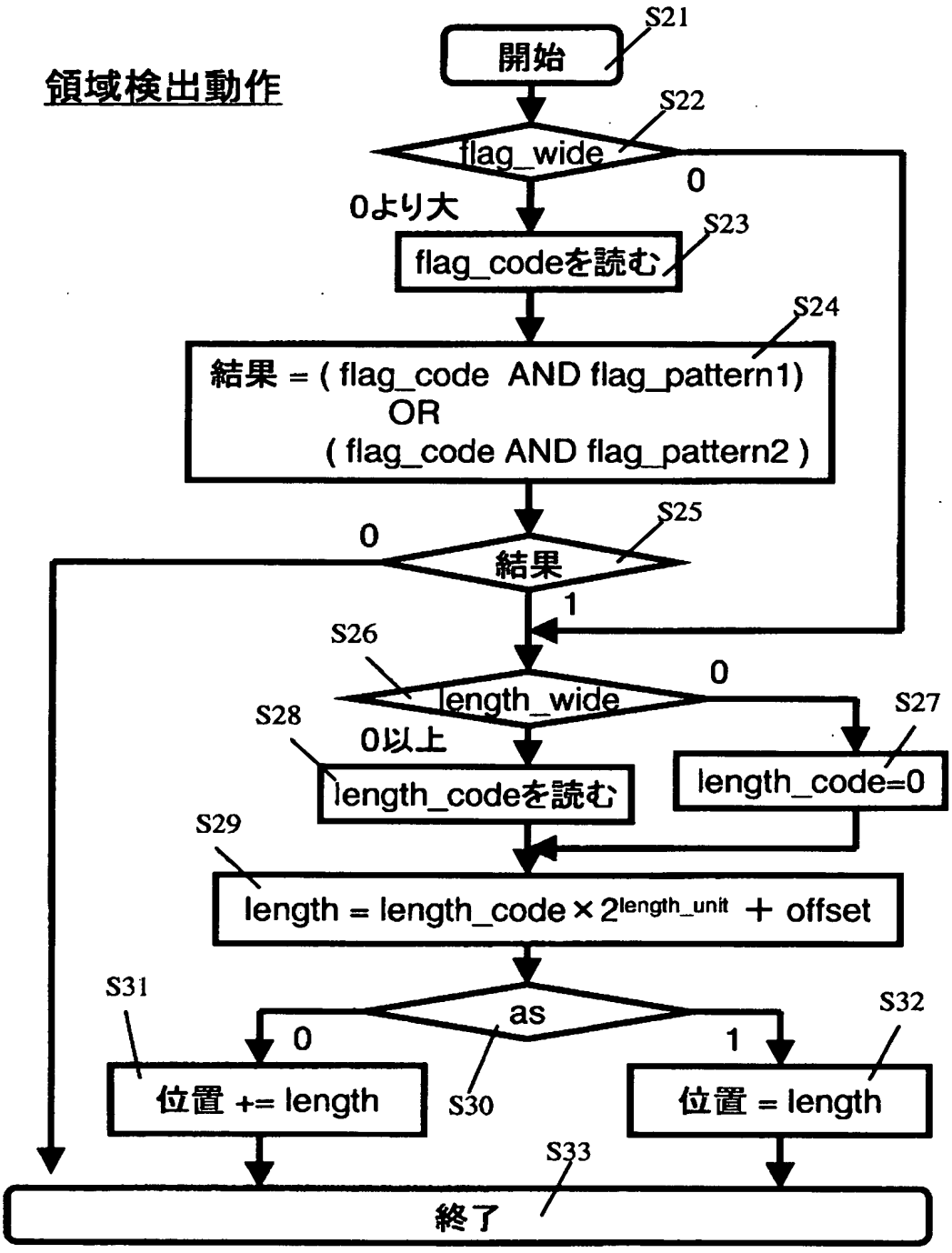
同期検証動作


S11
開始
S12
sync_wide
0
0より大
S13
同期チェック
S14
NG
結果?
S15
OK
smode=2
S16
エラー処理
S17
FALSEを返す
TRUEを返す
S18
終了
S19

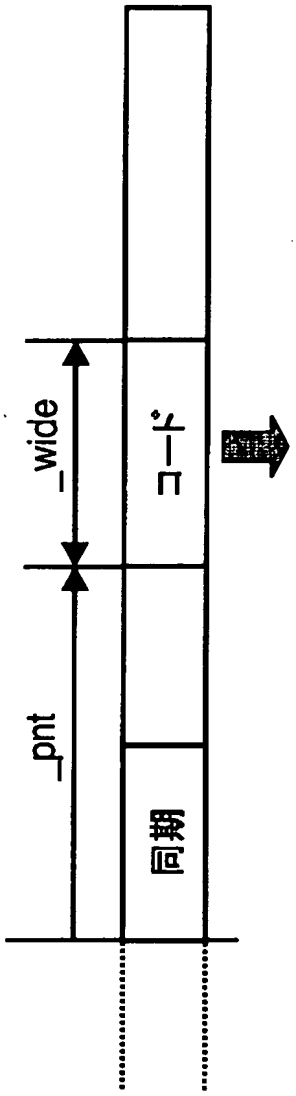
【図７】


31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
n
n+1
n+2
as
flag_wide
reserved
flag_pattern1
flag_pattern2
flag_pnt
offset
length_wide
length_type
length_unit
reserved
length_pnt

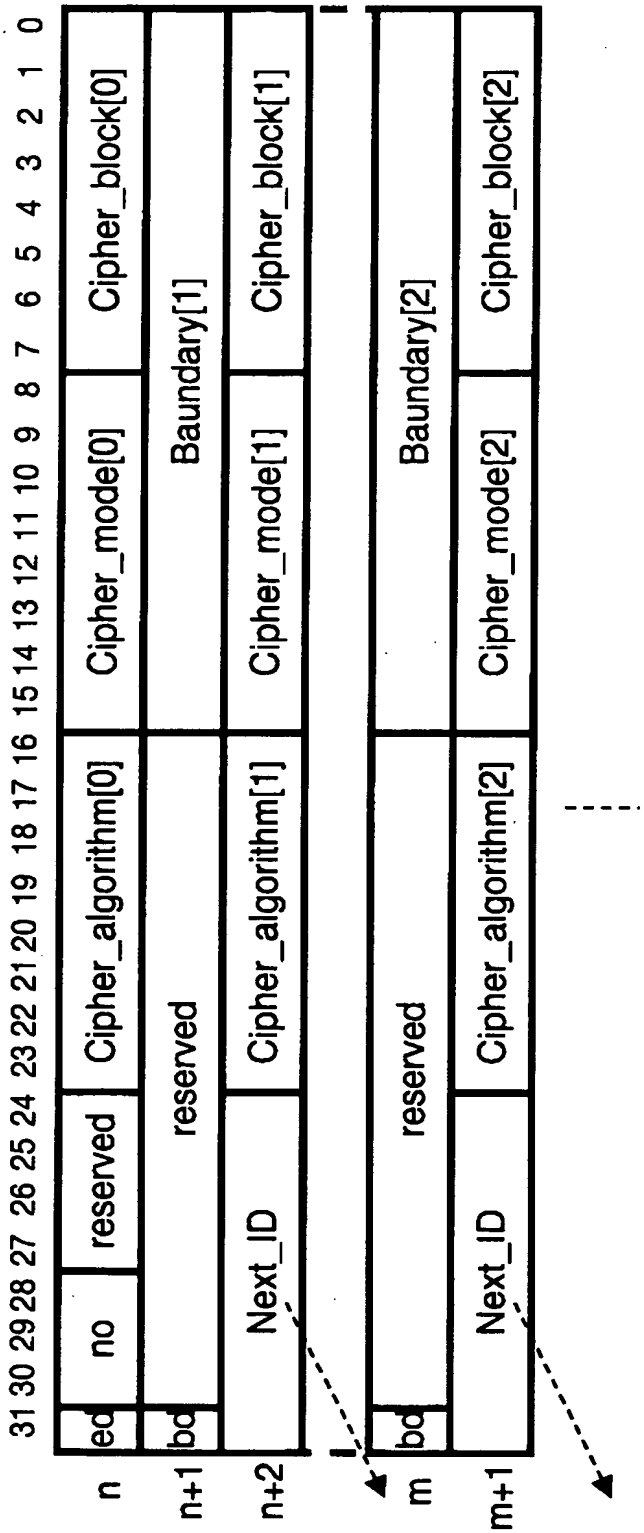
【図８】


領域検出動作
開始
S21
flag_wide
S22
0
0より大
flag_codeを読む
S23
S24
結果 = (flag_code AND flag_pattern1)
OR
(flag_code AND flag_pattern2)
0
結果
S25
1
S26
length_wide
0
S27
S28
0以上
length_codeを読む
length_code=0
S29
length = length_code × 2length_unit + offset
S31
as
S32
0
1
位置 += length
S30
位置 = length
S33
終了

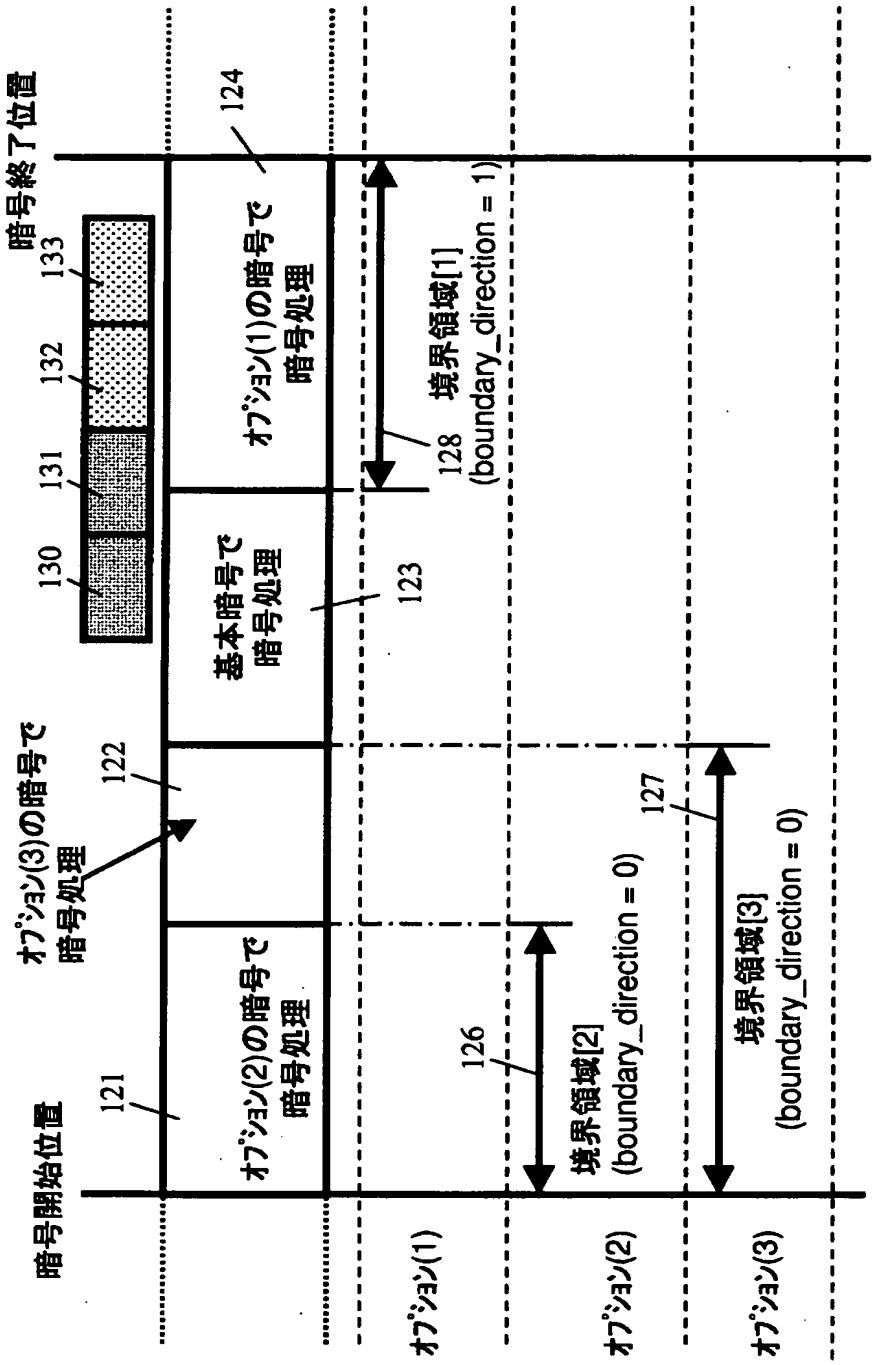
【図９】



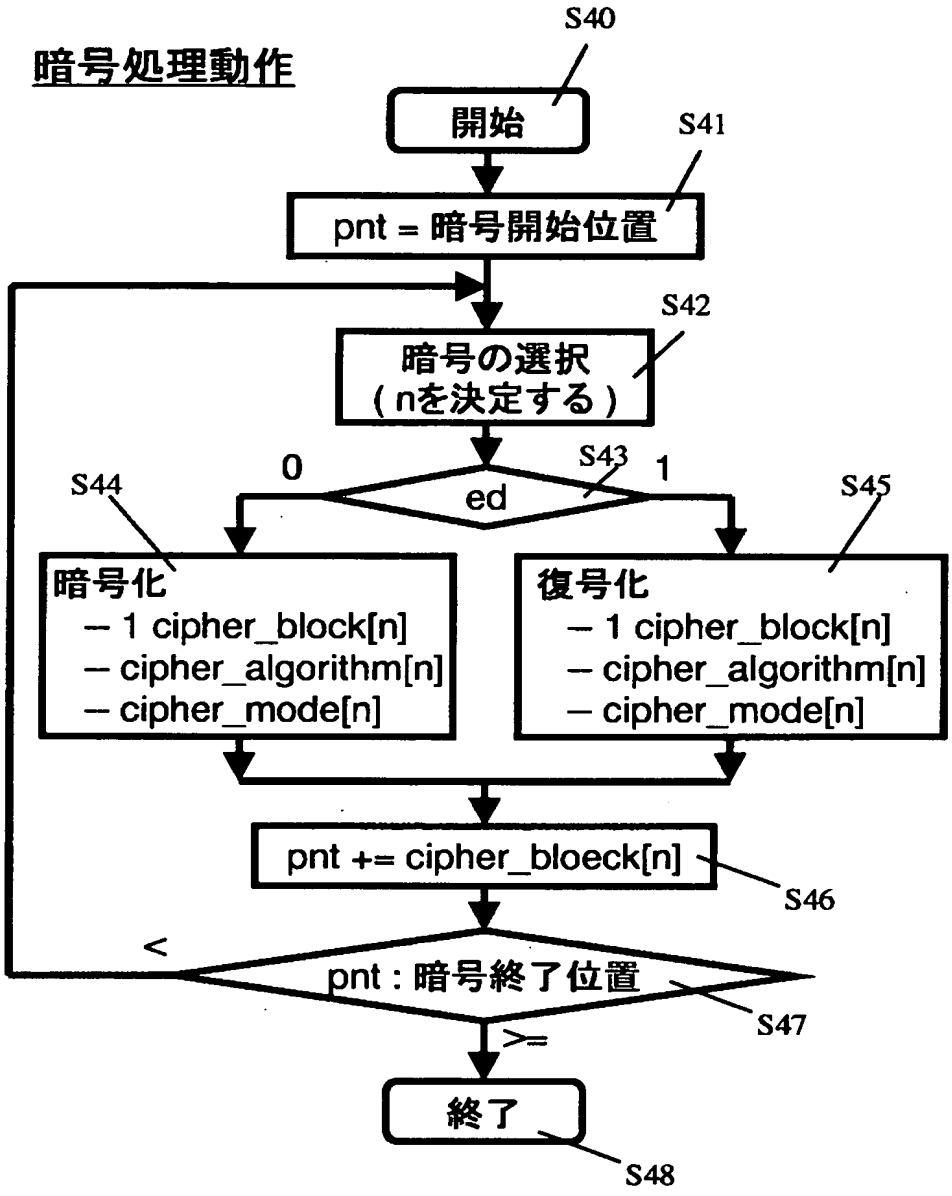
【図１０】


31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
ed
no
reserved
Cipher_algorithm[0]
Cipher_mode[0]
Cipher_block[0]
n
bd
reserved
Baundary[1]
n+1
Next_ID
Cipher_algorithm[1]
Cipher_mode[1]
Cipher_block[1]
n+2
bd
reserved
Baundary[2]
m
Next_ID
Cipher_algorithm[2]
Cipher_mode[2]
Cipher_block[2]
m+1

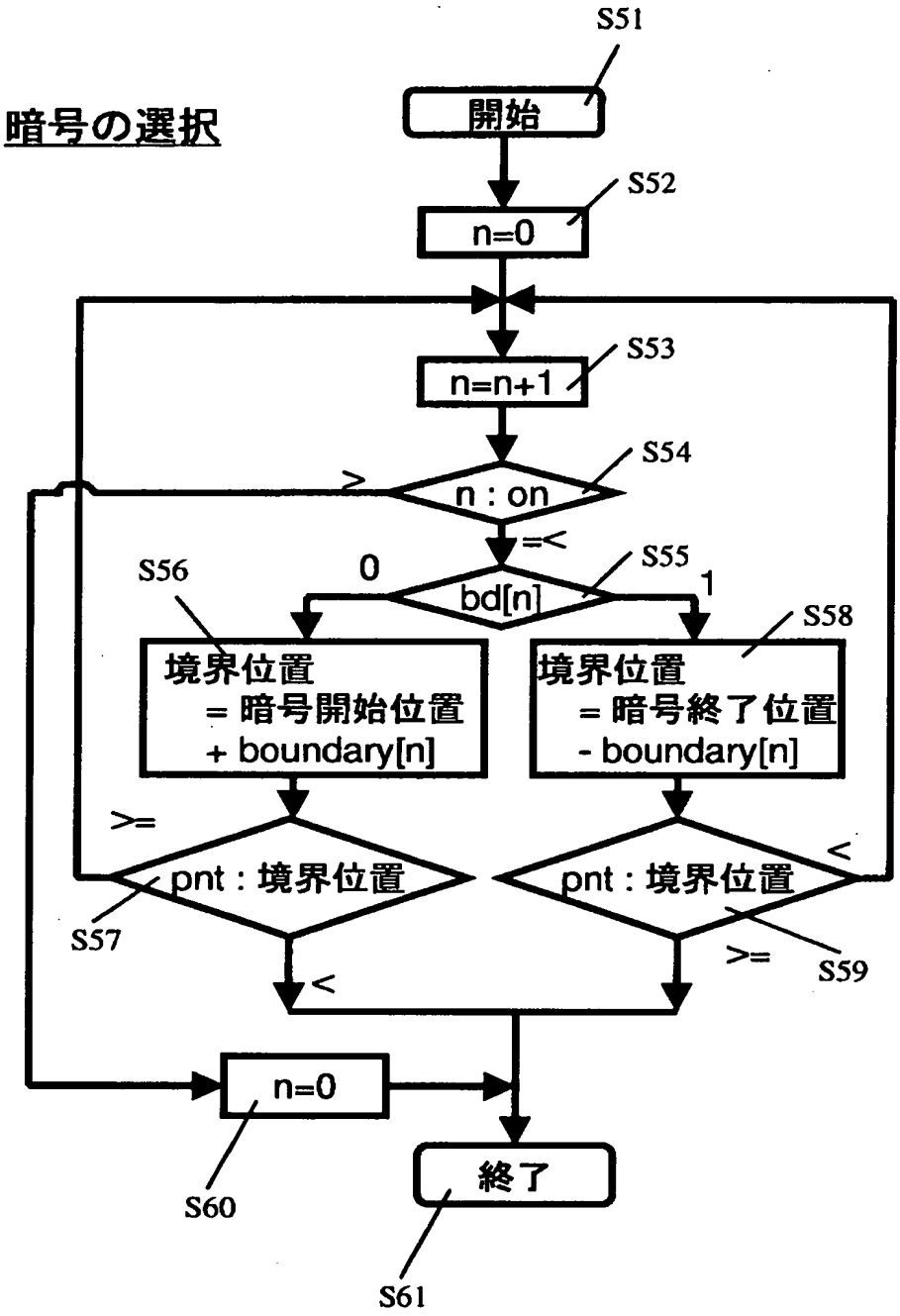
【図１１】


暗号終了位置
暗号開始位置
124
133
132
131
130
121
122
123
126
127
128
オプション(1)の暗号で暗号処理
基本暗号で暗号処理
オプション(2)の暗号で暗号処理
オプション(3)の暗号で暗号処理
境界領域[1] (boundary_direction = 1)
境界領域[2] (boundary_direction = 0)
境界領域[3] (boundary_direction = 0)
オプション(1)
オプション(2)
オプション(3)

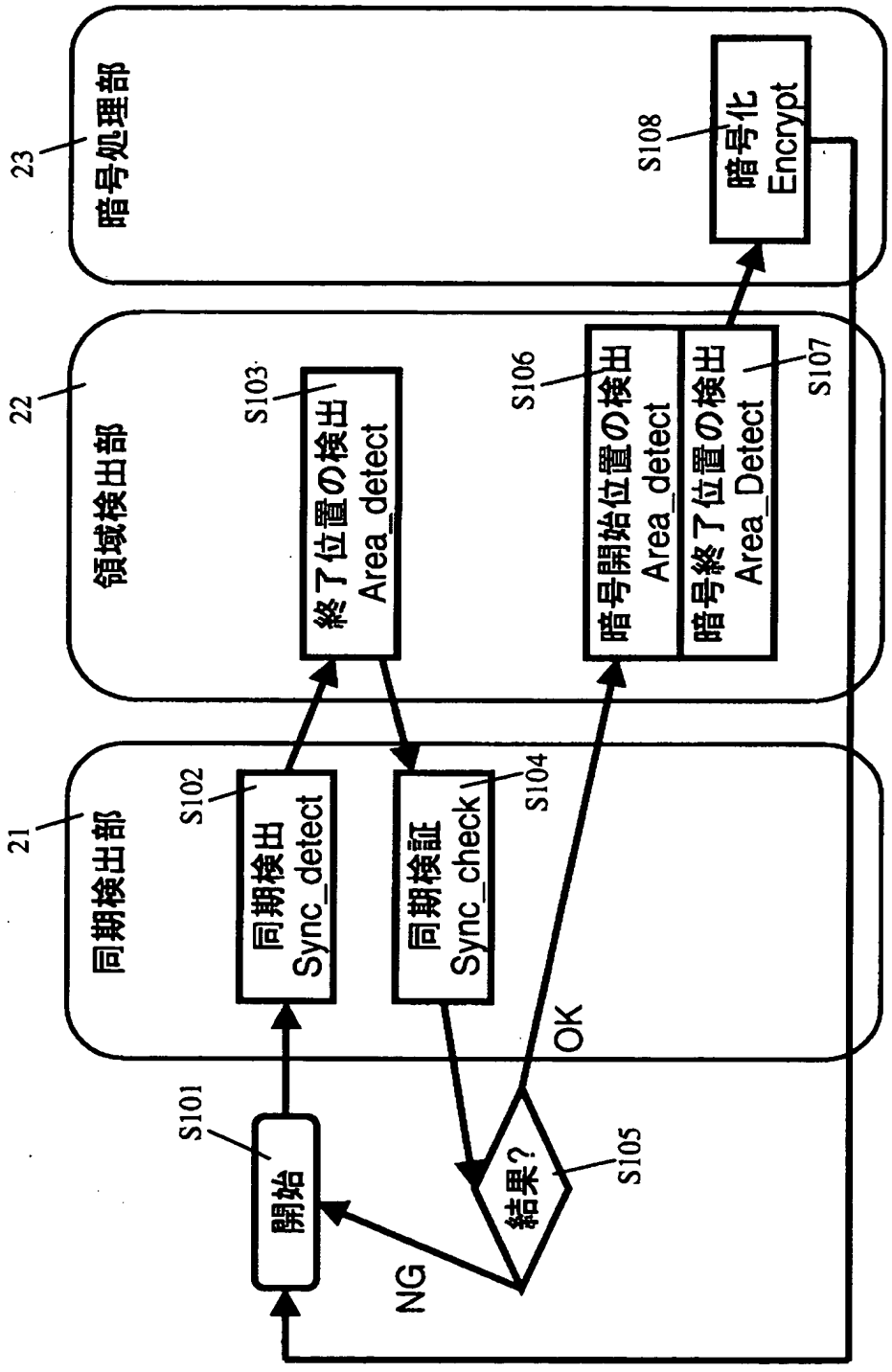
【図１２】


暗号処理動作
S40
開始
S41
pnt = 暗号開始位置
S42
暗号の選択
（nを決定する）
S43
ed
0
1
S44
暗号化
– 1 cipher_block[n]
– cipher_algorithm[n]
– cipher_mode[n]
S45
復号化
– 1 cipher_block[n]
– cipher_algorithm[n]
– cipher_mode[n]
pnt += cipher_bloeck[n]
S46
<
pnt : 暗号終了位置
S47
>=
終了
S48

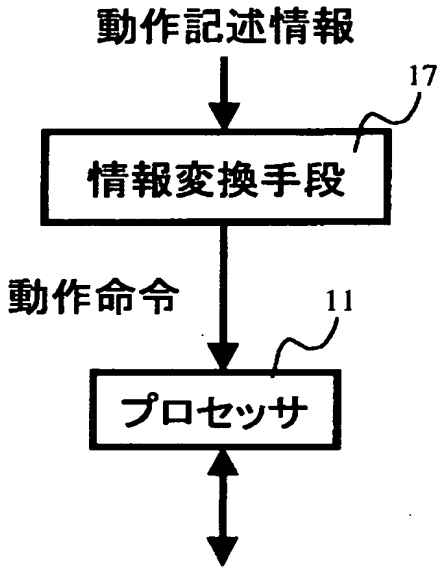
【図１３】


暗号の選択
S51
開始
S52
n=0
S53
n=n+1
S54
n : on
>
=<
S55
bd[n]
0
1
S56
境界位置
= 暗号開始位置
+ boundary[n]
S58
境界位置
= 暗号終了位置
- boundary[n]
>=
pnt : 境界位置
S57
<
pnt : 境界位置
>=
S59
<
n=0
S60
終了
S61

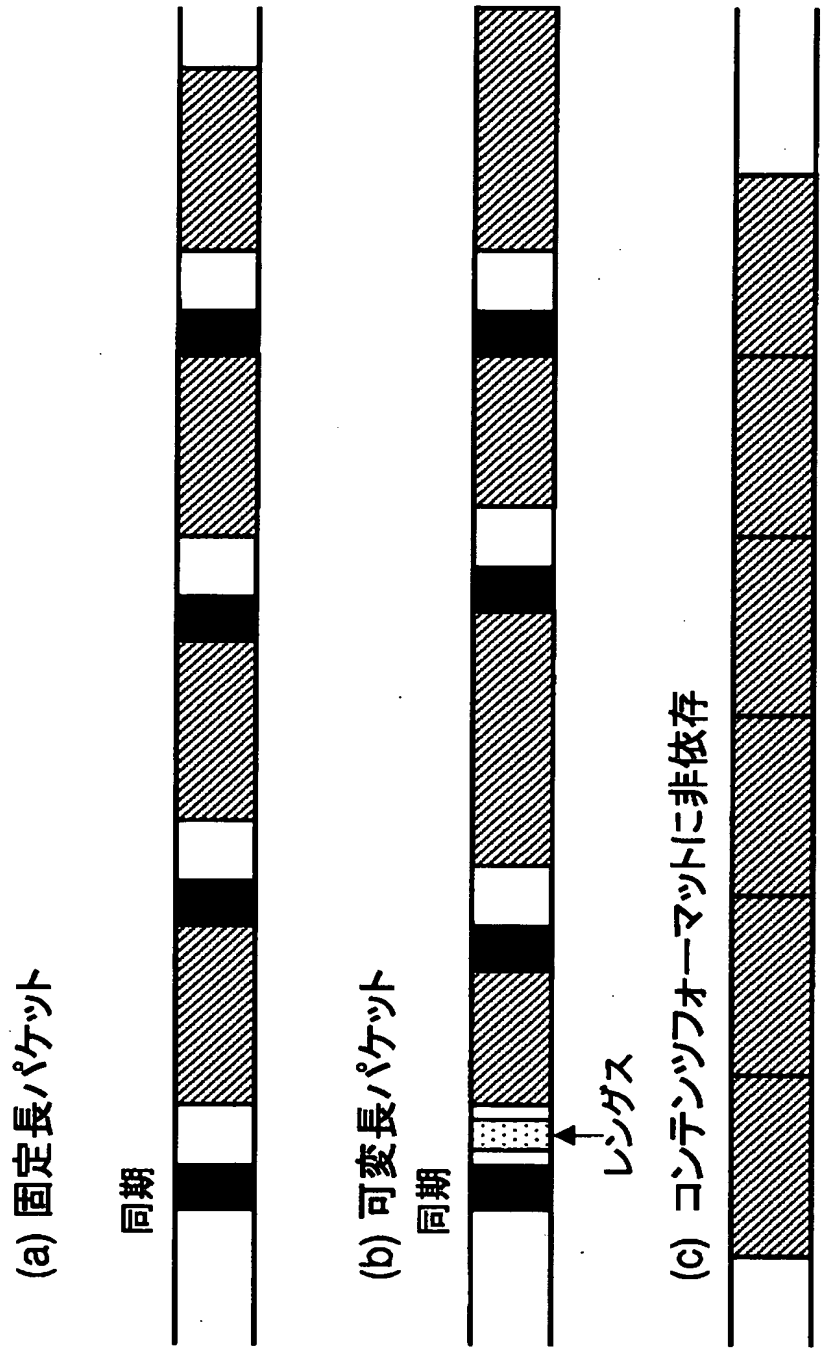
【図１４】


23
暗号処理部
S108
暗号化
Encrypt
22
領域検出部
S103
終了位置の検出
Area_detect
S106
暗号開始位置の検出
Area_detect
暗号終了位置の検出
Area_Detect
S107
21
同期検出部
S102
同期検出
Sync_detect
同期検証
Sync_check
S104
OK
S101
開始
結果?
S105
NG

【図１５】



【図１６】



【書類名】　要約書

【要約】

【課題】　任意のフォーマットのコンテンツへの暗号処理を実現できる暗号処理装置を構築する。

【解決手段】　コードの位置や長さなどを、動作記述言語で表現された動作記述情報をプロセッサ１１が処理し、各処理部を動作させる。同期検出部１２は同期位置の検出を行い、領域検出部１３は、暗号化開始や終了などの位置を検出する。暗号処理部１４は、暗号化開始と終了の間の領域を暗号処理する。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社